Enterprise Key and Certificate Management

Leaders in innovation, product features, and market reach for Enterprise Key and Certificate Management. Your compass for finding the right path in the market.

by Rob Newby
rn@kuppingercole.com
April 2014
Content Tables

Table 1: IBM Secure Key Lifecycle Manager major strengths and weaknesses .............................................. 19
Table 2: IBM Secure Key Lifecycle Manager rating ......................................................................................... 19
Table 3: Quintessence QCrypt major strengths and weaknesses ........................................................................ 20
Table 4: Quintessence QCrypt rating ................................................................................................................ 20
Table 5: RSA Data Protection Manager and Certificate Manager major strengths and weaknesses .......... 21
Table 6: RSA Data Protection Manager and Certificate Manager rating .......................................................... 21
Table 7: SafeNet DataSecure and KeySecure major strengths and weaknesses .............................................. 22
Table 8: SafeNet DataSecure and KeySecure rating .......................................................................................... 22
Table 9: Thales e-Security keyAuthority major strengths and weaknesses ..................................................... 23
Table 10: Thales e-Security keyAuthority rating ................................................................................................. 23
Table 11: Townsend Alliance Key Manager major strengths and weaknesses ............................................... 24
Table 12: Townsend Alliance Key Manager rating .......................................................................................... 24
Table 13: Venafi Director major strengths and weaknesses ................................................................................ 25
Table 14: Venafi Trust Protection Platform rating ............................................................................................. 25
Table 15: Vormetric DSM major strengths and weaknesses ............................................................................. 26
Table 16: Vormetric DSM rating ....................................................................................................................... 26
Table 17: Comparative overview of the ratings for the product capabilities .................................................. 27
Table 18: Comparative overview of the ratings for vendors ............................................................................ 27

Content Figures

Figure 1: Overall leaders in the EKCM market segment ................................................................................. 6
Figure 2: Product leaders in the EKCM market segment ................................................................................... 6
Figure 3: Market leaders in the EKCM market segment .................................................................................... 7
Figure 4: Innovation leaders in the EKCM market segment ............................................................................ 7
Figure 5: Market leaders in the EKCM market segment ................................................................................... 16
Figure 6: Product leaders in the EKCM market segment ................................................................................... 17
Figure 7: Innovation leaders in the EKM market segment ............................................................................. 18
Figure 8: The Market/Product Matrix ........................................................................................................... 28
Figure 9: The Product/Innovation Matrix .......................................................................................................... 30
Figure 10: The Innovation/Market Matrix ...................................................................................................... 31
Figure 11: Enterprise Certificate Management Matrix ................................................................. 32
Figure 12: EKM Matrix .................................................................................................................. 33
Figure 13: Overall leaders in the EKCM market segment .............................................................. 33

Related Research:

Executive View: Venafi Enterprise Key and Certificate Management - 70995
March 2014

Executive View: IBM Security Access Manager for Enterprise Single Sign-On - 71068
March 2014

Advisory Note: Enterprise Key and Certificate Management – 70885
January 2014

Leadership Compass: Enterprise Single Sign-On - 70962
January 2014

Vendor Report: SafeNet - 70876
October 2013

Snapshot: Vormetric Data Security - 70634
January 2013
1 Management Summary

Enterprise Key and Certificate Management (EKCM) is made up of two niche markets that are converging. This process still continues, and as with all major change of IT market segments, is driven by customer requirements. These customer requirements are driven by security and compliance needs. Up until recent times, compliance has been the bigger driver, but increasingly in the days of Cloud and mobile technology security of data in storage; data in the hands of others that is, security requirements have been brought to the fore.

The constituent parts of EKCM are Enterprise Key Management (EKM) and Enterprise Certificate Management (ECM).

ECM largely revolves around managing the keys from Public Key Infrastructures (PKIs); that is, creating, renewing, revoking the certificates, but also in this day and age, finding existing certificates and private keys within the corporate network. These certificates and keys can be used for encryption, authentication and message hashing.

EKM typically refers to the management of keys used for encryption and authentication their creation, rotation, revocation, retirement and archival. These are symmetric keys, and solutions have typically grown up as part of other product sets: Laptop, Application, Database, File, Disk, Fabric, Tape, Email and Mobile encryption solutions.

Each of these areas has its own issues in complexity and management to recognise and address, and the topic as a whole has overarching issues, which can affect data security if not handled properly. The two areas are already converging to address management issues, creating better usability and a consistent approach to both areas. Better security is inevitable when corporate secrets can be managed on an enterprise level rather than per technology.

It should be noted that Enterprise Key and Certificate Management (EKCM) is not solely about encryption. It is of course a large component of how and why keys and certificates are used, but it is not the be-all and end-all of EKCM. Certificates have multiple uses, as described in further in section 6.1, but the real crux of EKCM is efficient and reliable central management and monitoring of a diverse set of critical sensitive credentials to reduce overheads in other parts of the business, IT, helpdesk, security and HR to name those directly influenced.
A clear leader in almost every section, Venafi fare well in this Leadership Compass due to their leadership in this space. Almost uniquely, Venafi have chosen to combine Key and Certificate Management in one solution. There are a number of followers in this space, largely due to lack of development into the combined Key and Certificate Management solution set. SafeNet and RSA both have portfolios where this can be achieved, and scores were made based on separate certificate management and key management solutions, although their lack of integration was noted as a factor. The other vendors scored in this report either have the full solution scored together, or only offer one of the solutions in their portfolio.

Venafi lead in terms of Product for this very reason, but also in terms of continued development. Other products scoring lower in this section are not to be considered poor, or even lacking development, but not meeting the expectations of this LC. Quintessence Labs for example are clearly leaders in innovation, but this has yet to create a significant impression in the corporate market enterprise marketplace.
Vormetric have a large and effective development team, but their product set focuses on data security where Key Management is an optional add-on. These innovations may suit more academic approaches or those enterprises with specific requirements.

Figure 3: Market leaders in the EKCM market segment

Larger companies generally fare better in terms of market leadership, however results in this particular area are easily skewed in favour of smaller or privately owned vendors as financial data is often considered sensitive competitive information for larger vendors, and where they may be strong in reality, cannot be scored completely as a result.

As the space is still fragmented into ECM and EKM to a large extent, it is hard to state who has combined leadership of the market, but there is a clear leader of the combined market, in Venafi. Other vendors may have a stronger focus in either ECM or EKM, but Venafi clearly lead in both markets.

Figure 4: Innovation leaders in the EKCM market segment
There is a lot of innovation going on in this space, but there is still a chasm to cross for many vendors who are still concentrating on developing point solutions to become enterprise-ready. Whilst a well-developed application specific key manager can be turned into an enterprise key manager with relatively little trouble, this misses the certificate side of the solution, and this is where we find a number of the less developed solutions. Those who have traditionally played in the certificate space tend to be more advanced, simply because it is an easier journey from certificate management to key and certificate management than it is from just key management. To improve positioning within this LC, vendors should consider developing products in both areas of EKCM, combining them, ensuring effective central management and secure operations.

2 Methodology

KuppingerCole Leadership Compass is a tool that provides an overview of a particular IT market segment and identifies the leader in that market segment. It is the compass that assists you in identifying the vendors and products in a particular market segment which you should consider for product decisions.

It should be noted that it is inadequate to pick vendors based only on the information provided within this report. Customers must always define their specific requirements and analyze in greater detail what they need. This report does not provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

We look at four types of leaders:

- **Product Leaders**: Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what we expect from products in that market segment. They are mature.
- **Market Leaders**: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders**: Innovation Leaders are those vendors which are driving innovation in the particular market segment. They provide several of the most innovative and upcoming features we hope to see in the particular market segment.
- **Overall Leaders**: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in all areas.
For every area, we distinguish between three levels of products:

- **Leaders**: This identifies the leaders as defined above. Leaders are products which are exceptionally strong in particular areas or overall.
- **Challengers**: This level identifies products which are not yet leaders but have specific strengths which might make them leaders. Typically these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers**: This group contains products which lag behind in some areas, such as a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

In addition, we have defined a series of matrixes which:

- Compare the rating for innovation with the one for the overall product capabilities, thus identifying highly innovative vendors which are taking a slightly different path than established vendors, but also established vendors which don’t lead in innovation any more. These additional matrixes provide additional viewpoints on the vendors and should be considered when picking vendors for RfIs (Request for Information), long lists, etc. in the vendor/product selection process.
- Add views by comparing the product rating to other feature areas. This is important because not all customers need the same product, depending on their current situation and specific requirements. Based on these additional matrixes, customers can evaluate which vendor fits best to their current needs but also is promising regarding its overall capabilities. The latter is important given that a product typically not only shall address a pressing challenge but become a sustainable solution. It is about helping now and being good enough for the next steps and future requirements. Here these additional matrixes come into play.

Thus, the KuppingerCole Leadership Compass provides a multi-dimensional view on vendors and their products.

Our rating is based on a broad range of input and a long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

### 3 Product Rating

KuppingerCole as an analyst company regularly does evaluations of products and vendors. The results are, amongst other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.
KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

**Security** — security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

**Functionality** — this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

**Integration** — integration is measured by the degree in which the vendor has integrated the individual technologies or products in the portfolio. Thus, when we use the term integration, we are referring to the extent in which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

**Interoperability** — interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to insure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy) for more information about the nature and state of extensibility and interoperability.
Usability — refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, overall we have strong expectations regarding well integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes and breakdowns. This will create openings for attack and failure.

Thus when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided is of highest importance. This is because lack of excellence in any or all of these areas will lead to inevitable identity and security breakdowns and weak infrastructure.

4 Vendor Rating

For vendors, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are:

- Innovation
- Market position
- Financial strength
- Ecosystem

Innovation — this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the particular market segment(s) the vendor is in. Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. Driving innovation without standardization frequently leads to lock-in scenarios. Thus active participation in standardization initiatives adds to the positive rating of Innovation. Innovation, despite being part of the vendor rating, looks at the Innovation in the particular market segment analyzed in this KuppingerCole Leadership Compass.
**Market position** – measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active, e.g. being weak in one segment doesn’t lead to a very low overall rating. This factor takes into account the vendor’s presence in major markets. Again, while being part of the vendor rating, this mainly looks at the market position in the particular market segment analyzed in this KuppingerCole Leadership Compass. Thus a very large vendor might not be a market leader in the particular market segment we are looking at.

**Financial strength** – even while KuppingerCole doesn’t consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-funded are in general more likely to become an acquisition target, with massive risks for the execution of the vendor’s roadmap.

**Ecosystem** – this dimension looks at the ecosystem of the vendor for the particular product covered in this Leadership Compass document. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a “good citizen” in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

### 5 Vendor Coverage

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets like Germany, the US, or the APAC region.

However, there might be vendors which don’t appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Denial of participation:** Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular market segment.
- **Lack of information supply:** Products of vendors which don’t provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases we might decide not to include the product in that KuppingerCole Leadership Compass.
The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

For this Leadership Compass document, not all major vendors approached responded to the questionnaire: Hewlett-Packard, Oracle Corporation, Symantec and Cisco Systems declined to take part, despite having offerings in this space. There are also a number of point solutions in the market that have limited market visibility, so were not included in the leadership analysis for this KuppingerCole Leadership Compass: Cryptomathic, NetApp, Quantum Secure, Bell ID and Voltage fit into this category. These vendors are listed in section 15 of this document and might become part of the next edition of this document, depending on how they evolve.

### 6 Market Segment

Enterprise Key and Certificate Management (EKCM) is made up of 2 niche markets that are converging. This process still continues, and as with all products, is driven by customer requirements. These customer requirements are driven by security and compliance needs. Up until recent times, compliance has been the bigger driver, but increasingly in the days of Cloud and mobile technology security of data in storage; data in the hands of others that is, security requirements have been brought to the fore.

The constituent parts of EKCM are Enterprise Key Management (EKM) and Enterprise Certificate Management (ECM).

ECM largely revolves around what the industry has previously referred to as Public Key Infrastructure (PKI); that is, creating, renewing, revoking the certificates, but also in this day and age, finding existing certificates and private keys within the corporate network.

EKM typically refers to the management of keys used for encryption and authentication; their creation, rotation, revocation, retirement and archival. These are symmetric keys, and solutions have typically grown up as part of other product sets: Laptop, Application, Database, File, Disk, Fabric, Tape, Email and Mobile encryption solutions.

The main difference between the 2 approaches therefore is the type of keys under consideration.

#### 6.1 Enterprise Certificate Management Features

ECM takes asymmetric (public and private) keys and their associated certificates into account. ECM could be considered part of Public Key Infrastructure (PKI), which typically takes the registration of users, creation and revocation of certificates and their management into account, but not discovery and management of certificates and keys within a corporate environment. Other aspects of the management of certificates include user credential and token management but are not normally considered part of enterprise certificate management. This is why vendors such as Bell ID, gemplus, G&D, Actividentity do not fit into this ECM report. Most people think of ECM as provisioning certs to server based apps or standalone devices/appliances rather than user level certs and tokens or smart cards.
ECM does not usually include its own certificate authority, or therefore root CA and registration authority. Automatic location of certificates and retrieval of private keys is a valuable feature of the product set as replacing these takes a lot of time and effort.

Private keys are used for encryption (e.g. S/MIME email) and are associated with certificates used for identification. Public keys associated with this type of infrastructure are also used for hashing of messages for integrity. Private keys can be simply protected in hardware using hardware security modules (HSMs) for servers and TPMs (Trusted Platform Modules) for desktops. Public keys do not need protecting, as the security of the system is guaranteed by the private key. Although secure, the decryption of messages encrypted with private keys is computationally expensive.

6.2 Enterprise Key Management Features

EKM is the management of symmetric keys; the same key is used for encryption and decryption. Rapid retrieval of these keys is vital for data access, but management of these keys also takes into account actions such as revocation and rotation. A major difference of the EKM product set is that key retrieval is of lesser value where they can be easily replaced, although most solutions include a key vaulting solution which is the source of key archival in the organisation. Many products claiming to be EKCM do not have key retrieval functionality, which quickly identifies them as not yet belonging in this market.

Symmetric keys are more simply applied in encryption and decryption operations (e.g. file encryption), and as such create a far lower computational overhead at each end of an encrypted transaction. However, systems which use symmetric keys would be exposed if these keys were intercepted, so these are often protected using asymmetric keys, creating a hybrid cryptosystem – the more easily secured asymmetric encryption protecting the faster symmetric encryption keys.

Most platforms which call themselves EKM only today will certainly have another layer of certificate/private key based protection on top to protect access to the symmetric keys within the system. Once these key management devices were created, it was a matter of integrating with other standalone products that had appeared such as individual key managers for tape libraries and email.

It is noteworthy however that virtually all EKM systems are physically hardened appliance-based products and most ECM products are purely software based products. It is certainly easier for EKM products to add the functionality for managing certificates than it is for ECM products to bolster their native security posture to be trusted with symmetric private keys.

6.3 Enterprise Key and Certificate Management

It can be seen then that the main difference between the two approaches is the type of keys under consideration. This leads to a difference in strategy when deploying, but with similarities which are ensuring that these two key management systems are converging in both approach and technology. Where there are different technical reasons for deploying asymmetric and symmetric keys, the security of them is paramount, and as such the management of them must be done to the same standards, and with the same separation of duties. Key lifecycles must be understood in correct context, access and ownership must be carefully managed.
EKCM makes all of these features available in one centrally managed and monitored resilient system, enabling rapid expansion of any set of keys, management of large numbers of certificates, renewal and replacement on an enterprise scale. Each area of EKCM presents its own issues, and some areas are found in both, which create the basis for a common strategic approach. This market is fairly new however, and most vendor offerings are still either still in separate products, or remain as point solutions in the EKM space.

7 Specific Features Analyzed

When evaluating these products, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- platform support

We also looked at:

**Enterprise readiness** Whether Key and Certificate Management was effectively merged, and a combination of the elements required for Enterprise – support and licensing in particular.

**Ease of installation** The solution delivery method (i.e. appliance/software/hardware) and how it integrates in an Enterprise environment. In situations where complexity was a factor, the availability of Professional Services.

**Secure Management** Specific EKCM management items such as key and certificate lifecycle. Also areas of the product enabling secure integration and usability. Following security best practice is expected in this area as a baseline requirement.

**Secure Operations** Support for types of keys and ensuring security in operation, including data and key protection and the logging and monitoring interface.

As the popularity of Cloud computing increases, protection of sensitive corporate information is becoming a more widespread and important issue. This requires encryption, both symmetric and based on public key approaches. Setting up a well-defined approach to managing keys and certificates, based on well-defined corporate guidelines is an issue often avoided, and therefore managed at a tactical level. Enterprise PKIs, email encryption solutions, flat file and database encryption systems are all established technologies, however the need for EKM is still not well understood at a corporate level. Thus, implementation rates are still rather low. We expect a strong increase in this market segment within the next 24 to 36 months due to the need for ubiquitous encryption in the light of the increase in Information Security Risks and Cyber Espionage.
8 Market Leaders

Based on our evaluation of the products, we identified (as mentioned above) different types of leaders in the EKM market segment. The market leaders are shown in

![Market Leaders Diagram]

Figure 5: Market leaders in the EKCM market segment

The market is affected by a situation where several very large software vendors compete with a large number of smaller vendors. Market leadership is mainly a hint at the overall position of the vendor regarding the number and size of customers, its strength in sales, and its partner ecosystem.

We expect Market Leaders to be leaders on a global basis. Companies which are strong in a specific geographic region but sell little or nothing to other major regions are not considered market leaders. The same holds true for the vendor’s partner ecosystem – without global scale in the partner ecosystem, we do not rate vendors as Market Leaders.

Market Leadership is an indicator of the ability of vendors to execute on projects. However, this depends on other factors as well. Small vendors might well be able to execute in their “home base”.

Small vendors are sometimes more directly involved in projects, which can be positive or negative – the latter, if it leads to branches in product development which is not managed well. It should be noted that position in this chart can often be relative to size however. Townsend notably fare well in this regard due to good coverage and successful projects for a relatively small company. Besides that, the success of projects depends on many other factors, including the quality of the system integrator – so even large vendors with a good ecosystem might fail in projects. It has to be noted that this Market Leadership rating does not allow any conclusion about whether the products of the different vendors fit the customer requirements.

Market Leaders are (in alphabetical order)

- IBM
- RSA
- Townsend
- Venafi

KuppingerCole Leadership Compass
Identity Provisioning
Report No.: 70949
9 Product Leaders

The second view we provide is about product leadership. That view is mainly based on the analysis of product features and the overall capabilities of the various products.

Here it has to be noted that several products that appear more to the left side frequently gained their rating because they take different approach to EKCM from the leading vendors.

Quintessence Labs are a spin-off from NASA, and as such have an impressive innovation portfolio, but this may be too forward thinking for many real-world customers. Venafi, on the other hand, have the only truly integrated EKCM device currently on the market, which explains their position in our view. Most vendors are sitting in the middle of these two extremes, with either separate products, or a single product which addresses a niche, but is being developed. RSA, for example, have RSA DPM for the purposes of key management, but also have separate certificate management and key discovery products, not yet integrated with DPM. It is unclear at this stage (to RSA) whether they have a requirement to combine. For the purposes of this report, this has been considered in the scoring.

Again, to select a product it is important to look at the specific features and map them to the customer requirements. There are many examples where products that are not “feature leaders” are still the better fit for specific customer scenarios.

Product Leaders are (in alphabetical order):

- RSA
- Safenet
- Thales
- Venafi
10 Innovation Leaders

The third angle we took when evaluating products was about innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require to receive new releases that meet new requirements. Thus, a look at innovation leaders is also important, beyond analyzing product features.

![Figure 7: Innovation leaders in the EKM market segment](image)

Again, in some cases products that appear more to the left of that figure do not necessarily fail in innovation but are focused on specific requirements or highly focused approaches. IBM are still largely focused around encryption of their own DB/2 databases, which is to be expected, although does not create a good score in this case.

Quintessence Labs are notable in this segment, with some very exciting research into Quantum Cryptography not covered by this LC, but worth an honourable mention and influencing the scoring significantly. They and the other “Leader” vendors have demonstrated a significant amount of innovation in recent time, driving standards evolution of this space forwards.

Innovation Leaders are (in alphabetical order):

- RSA
- Safenet
- Venafi

11 Product Evaluation

This section contains a quick rating for every product we’ve included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and KuppingerCole Executive View Reports available, providing more detailed information.
11.1 IBM Secure Key Lifecycle Manager

IBM’s focus is on usability, with a relatively limited product in terms of functionality. Having said this, all of the required features are present for the purpose of flat file encryption – used for the encryption of IBM DB/2 database files to good effect. This is a case of a good point product scoring well amongst other enterprise products, despite falling short on certificate functionality.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Well recognized industry name</td>
</tr>
<tr>
<td>• Reliable key management software</td>
</tr>
<tr>
<td>• Large existing client-base</td>
</tr>
<tr>
<td>• Integrates seamlessly with IBM DB/2 databases</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Limited key functionality</td>
</tr>
<tr>
<td>• No certificate functionality</td>
</tr>
</tbody>
</table>

Table 1: IBM Secure Key Lifecycle Manager major strengths and weaknesses

IBM are supporting KMIP and planning to extend the functionality of the product to cover more endpoints/applications, hence their inclusion in this LC. In certain situations, existing DB/2 customers that is, this encryption is certainly to be recommended, although this will not currently stack up against the enterprise key and certificate managers in the market currently.

<table>
<thead>
<tr>
<th>Security</th>
<th>neutral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>weak</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>neutral</td>
</tr>
<tr>
<td>Usability</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 2: IBM Secure Key Lifecycle Manager rating

It is unlikely that IBM plan to become a leader in EKCM, however if there is an aim for improvement in this area as indicated by their extension of KMIP, they should consider developing their free certificate manager into an enterprise offering, and combine management of both.
11.2 Quintessence QCrypt

Quintessence provide a common administration interface across multiple end-point systems for central policy control. This enables all operations to be logged in a central audit trail.

Key material is securely replicated to ensure high availability and redundancy, also allowing scaling to manage very large numbers of keys and clients across multiple domains, with either peer or delegated responsibilities. Key support and management is generally good, including support for one-time pad key material, random objects and streams.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Interoperable with multiple vendors through OASIS KMIP standard</td>
<td>• Lack of global presence</td>
</tr>
<tr>
<td>• End-to-end life cycle management of keys based on NIST SP 800-57 Part 1 guidelines</td>
<td>• Small number of vendor partnerships</td>
</tr>
<tr>
<td>• Cutting edge development is interesting to follow and write about</td>
<td>• Cutting edge development may be too much for corporates to understand</td>
</tr>
</tbody>
</table>

Table 3: Quintessence QCrypt major strengths and weaknesses

Again, as an encryption and key management solution, QCrypt performs well, and has some impressive technology, but overall lack certificate management, as well as the global coverage, integration and partnerships required to improve profile and coverage in the market.

Hardware based gigabit per second full entropy, a non-deterministic random number generator with quantum derived entropy source and optional quantum key distribution link for server-to-server replication all sound like options worth investigating, but Quintessence need to be careful not to blind the market with science.

<table>
<thead>
<tr>
<th>Security</th>
<th>positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>neutral</td>
</tr>
<tr>
<td>Integration</td>
<td>neutral</td>
</tr>
<tr>
<td>Interoperability</td>
<td>neutral</td>
</tr>
<tr>
<td>Usability</td>
<td>weak</td>
</tr>
</tbody>
</table>

Table 4: Quintessence QCrypt rating

QCrypt is broad-based enough to not need a lot of further development within the EKM space, but addition of Certificate Management would aid further progression in this market.
11.3 RSA Data Protection Manager and Certificate Manager

RSA Data Protection Manager has grown up from RSA Enterprise Key Manager, and added features as it has developed. The major addition to Key Management has been tokenization. On top of very reliable enterprise level Key Lifecycle Management, this makes RSA a leading contender in the EKM market. RSA Certificate Manager has been in the market since 2000, making it one of the most mature offerings available.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Well recognized industry name</td>
<td>• Roadmap has developed very quickly over the past few years, could be leaving</td>
</tr>
<tr>
<td>• Reliable key management software</td>
<td>potential new customers confused and overwhelmed</td>
</tr>
<tr>
<td>• Large existing client-base</td>
<td>• Relatively small specialized partner</td>
</tr>
<tr>
<td>• Integration with existing RSA products</td>
<td>ecosystem and professional services</td>
</tr>
<tr>
<td>• Internal and external communications</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: RSA Data Protection Manager and Certificate Manager major strengths and weaknesses

It should be noted that RSA do not combine their Certificate Management with Data Protection Manager, but offer good interoperability. This is a deliberate strategy, keeping the offerings available as part of focused solutions. This helps them to differentiate between key management and certificate management, but may also create confusion amongst customers unless properly explained. To their credit, RSA are a customer focused company who spend a lot of time working out customers’ real needs before guiding them to a decision and they certainly have the internal resources available to create these explanations

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 6: RSA Data Protection Manager and Certificate Manager rating

The Data Protection Manager is a good EKM product which should be combined with RSA Certificate Manager to cover the EKCM space. Further enterprise development could see this as a strong contender in this market.
11.4 SafeNet DataSecure and KeySecure

SafeNet has a good, solid reputation in the HSM business. The SafeNet portfolio has been expanded largely by acquisition which has allowed significant portfolio expansion in a short timeframe, but this has brought with it issues around product maturity and integration. KeySecure and DataSecure are both very detailed products, which have support for multiple platforms and applications. The concern is that support of these could overstretch the development of the product overall.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Flexible deployment, virtual or Safenet hardware</td>
<td>• Products are not integrated with each other in the overall portfolio</td>
</tr>
<tr>
<td>• Broad ecosystem</td>
<td>• Standalone product maturity is generally good but could slip due to multi-faceted nature of products</td>
</tr>
<tr>
<td>• Layered Encryption product support</td>
<td></td>
</tr>
<tr>
<td>• KMIP/ICAPI client</td>
<td></td>
</tr>
<tr>
<td>• PKCS#11 (C/C++), JCE (Java), .Net client support</td>
<td></td>
</tr>
</tbody>
</table>

Table 7: SafeNet DataSecure and KeySecure major strengths and weaknesses

SafeNet are masters of the security story however, and will continue to make progress in any direction where their customers want this to go. The DataSecure and KeySecure solution set is well described and well understood internally and integrates well with other products.

<table>
<thead>
<tr>
<th>Security</th>
<th>positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>neutral</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 8: SafeNet DataSecure and KeySecure rating

The DataSecure product includes KeySecure functionality and is the managing platform behind ProtectApp, ProtectDB, ProtectFile, and Tokenization Manager products. It manages the entire encryption product line. KeySecure is used as the key manager or StorageSecure (ex-NetApp product), as well as ProtectV. KeySecure has a large number of integration partnerships compared to other key management providers. Promised near-term integration of DataSecure and KeySecure under a common management and reporting function will make them one of the strongest contenders in the market.
11.5 Thales e-Security keyAuthority

Many of the devices in this LC claim FIPS 140-2 validation, but keyAuthority has FIPS 140-2 Level 3 validation for the whole device chassis, support for KMIP 1.2 and policy enforcement making it one of the most secure offerings in the LC. Policies include role-based access control, multi-factor authentication, secure audit facilities, master key quorum and two-person rules. All of these are good solid product features, and create good scores across the board, particularly in security, integration and usability. However, apart from its good scalability, there is nothing outstanding about the keyAuthority product to help it in a head to head situation with other products.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Well recognized industry name</td>
<td>• Lack of real unique selling point amongst competition</td>
</tr>
<tr>
<td>• Good reputation in HSM space</td>
<td></td>
</tr>
<tr>
<td>• Reliable key management software</td>
<td></td>
</tr>
<tr>
<td>• Large existing client-base</td>
<td></td>
</tr>
</tbody>
</table>

Table 9: Thales e-Security keyAuthority major strengths and weaknesses

Thales calls out pre-qualification with client devices and endpoints for simpler customer deployment, which should not be underestimated, however this can be a downside in terms of product development. There are of course situations where keyAuthority will be the best product based on specific requirements. Thales have concentrated hard on providing very secure key management products, and this has paid off in many vertical markets – government and financial institutions have benefitted from their hardware for many years.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>neutral</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 10: Thales e-Security keyAuthority rating

Now that Thales have a good reputation for security, they would be well served to concentrate on developing the functionality and management of their devices. As with many products in this space, development of Certificate Management would improve overall functionality, as long as management of the device stays mature and secure.
11.6 Townsend Alliance Key Manager

Townsend advertise the Alliance Key Manager as the only key management solution providing support for IBM DB/2 fieldproc on the IBM I platform. This begs the question as to why IBM do not provide this support themselves when they are providing a DB/2 encryption solution. IBM take a different approach to encryption, encrypting the DB/2 flat file in storage. This is not a key management issue however.

Both approaches require agent software, and as such there is no obvious benefit in one approach or other. There is no charge for client side licenses from Townsend however.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• KMIP support</td>
<td>• Small company</td>
</tr>
<tr>
<td></td>
<td>• Point solution for database encryption</td>
</tr>
<tr>
<td></td>
<td>• No certificate management</td>
</tr>
</tbody>
</table>

Table 11: Townsend Alliance Key Manager major strengths and weaknesses

The next release of Alliance Key Manager is touted to provide full lifecycle key management, on-device encryption services, support for Microsoft SQL Server encryption, real-time full duplex key mirroring and support for cloud environments. These are all good moves towards a stronger key management solution, but does not move it into the certificate management space.

<table>
<thead>
<tr>
<th>Security</th>
<th>neutral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>neutral</td>
</tr>
<tr>
<td>Integration</td>
<td>neutral</td>
</tr>
<tr>
<td>Interoperability</td>
<td>neutral</td>
</tr>
<tr>
<td>Usability</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 12: Townsend Alliance Key Manager rating

Townsend are in a very niche product area, which they serve well. They do not seem to suffer from much competition in their chosen area, but it is only a matter of time until their products are superseded by features of other product sets. They would be advised to broaden the reach of their product set and take advantage of more partnerships, perhaps with a view to acquisitions to expand their reach.
11.7 Venafi Trust Protection Platform

The only single product in this LC to combine key and certificate management effectively on one platform and allow customers to choose functionality from a range of available solutions in one central place.

Venafi came from an ECM background to become a market leader in their field. Their main competition evolved from EKM devices and HSM manufacturers’ acquisition and consolidation of products. As a result Venafi has a well-developed software solution in the EKCM space which has all of the functionality that would be expected from a niche market leader, hardware protection is optional and at customer discretion. Venafi supports HSMs from Thales and SafeNet. All of the required management functionality is available in a centralised software-based console.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• True enterprise product</td>
<td>• Limited overall product set as a vendor</td>
</tr>
<tr>
<td>• Combined key and certificate management</td>
<td>• Little room for improvement in this set may cause stagnation</td>
</tr>
<tr>
<td>• Well-developed product</td>
<td></td>
</tr>
</tbody>
</table>

Table 13: Venafi Trust Protection Platform major strengths and weaknesses

With a lot of financial backing and market success, it would easy for Venafi to remain safe and not venture out of the market which they clearly excel in. Indeed, this may be the direction they are encouraged in by their many backers and advisers, who have spent time and money developing a security background story and go to market strategy.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>strong positive</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 14: Venafi Trust Protection Platform rating

Any search on the web that includes key or certificate management is practically guaranteed to come up with a link to the Venafi website, particularly when referred to as EKCM. Venafi has positions itself well in this market, and clearly knows which way it is heading. Over the last 3-4 years, they have clearly honed their go to market plan, and have a strong security story behind them.

An impressive market leader, but in today’s security market, small companies like Venafi need to keep moving forwards and, more importantly, be seen to be improving, growing in size/coverage or expanding their portfolio to retain profitability and profile.
11.8  Vormetric Data Security Manager (DSM)

Vormetric’s focus is on simplifying data security across cloud, virtual, big data and traditional environments. Their cornerstone product Vormetric Transparent Encryption is an agent that runs at the filesystem level and receives policies and keys from the DSM. This solution gives benefits over full-disk encryption solutions because they have context to provide fine grained access control with encryption. At the same time it gives advantages over application-level encryption because there is no integration to be performed. This enables transparent Cloud deployments, and they have several successful deployments in this area. Additionally, when the need for field-level encryption is required, Vormetric offers the Vormetric Application Encryption product, which shares the same DSM for key and policy management. It is only recently they began expanding into the EKM market, TDE Key Management support was added in 2012 and in 2013 Vormetric added Certificate Inventory, KMIP Support, and opened their PKCS#11 API.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Filesystem level encryption makes the encryption largely application independent</td>
<td>• Lacks certificate management, offering is more certificate inventory and secure storage, so may be overtaken in head to head situations where a combined key and certificate management solution is required.</td>
</tr>
<tr>
<td>• KMIP and PKCS#11 support</td>
<td></td>
</tr>
<tr>
<td>• Strong partnerships with other large vendors spreads the exposure of Vormetric in the market</td>
<td></td>
</tr>
</tbody>
</table>

Table 15: Vormetric DSM major strengths and weaknesses

Vormetric spend a lot of time on development, and know what customers are looking for with an encryption solution. They therefore offer extensive platform support, privileged user access control, separation of duties, logging/auditing, and centralized management. As an EKM solution, they perform satisfactorily, and can meet specific customer requirements better than other solutions due to their unique approach to encryption. It is important to note that the Vormetric solution fits into other data security and encryption markets, not just EKCM.

<table>
<thead>
<tr>
<th>Security</th>
<th>positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>neutral</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>neutral</td>
</tr>
</tbody>
</table>

Table 16: Vormetric DSM rating

To excel in EKM, Vormetric needs to add a richer set of certificate life cycle management capabilities to their offering. Vormetric has a clever solution to file-level and database encryption, privileged user access control, security intelligence and application-level encryption libraries. They have solid KMIP and PKCS#11 support and proven interoperability, however, they require additional investment in certificate management to be a leader in this space.
12 Products at a Glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 17.

<table>
<thead>
<tr>
<th>Product</th>
<th>Security</th>
<th>Functionality</th>
<th>Integration</th>
<th>Interoperability</th>
<th>Usability</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Secure Key Lifecycle Manager</td>
<td>neutral</td>
<td>weak</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
</tr>
<tr>
<td>Quintessence QCrypt</td>
<td>positive</td>
<td>neutral</td>
<td>neutral</td>
<td>neutral</td>
<td>weak</td>
</tr>
<tr>
<td>RSA Data Protection Manager and Certificate Manager</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
</tr>
<tr>
<td>SafeNet DataSecure and KeySecure</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
<td>neutral</td>
<td>strong positive</td>
</tr>
<tr>
<td>Thales eSecurity keyAuthority</td>
<td>strong positive</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
<td>positive</td>
</tr>
<tr>
<td>Townsend Alliance Key Manager</td>
<td>neutral</td>
<td>neutral</td>
<td>neutral</td>
<td>neutral</td>
<td>positive</td>
</tr>
<tr>
<td>Venafi Trust Protection Platform</td>
<td>strong positive</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Vormetric DSM</td>
<td>positive</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
<td>neutral</td>
</tr>
</tbody>
</table>

Table 17: Comparative overview of the ratings for the product capabilities

In addition we provide an overview in Table 18 which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Innovation</th>
<th>Market Position</th>
<th>Financial Strength</th>
<th>Ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM</td>
<td>weak</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Quintessence</td>
<td>positive</td>
<td>positive</td>
<td>neutral</td>
<td>neutral</td>
</tr>
<tr>
<td>RSA</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
<td>positive</td>
</tr>
<tr>
<td>SafeNet</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
</tr>
<tr>
<td>Thales</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
</tr>
<tr>
<td>Townsend</td>
<td>neutral</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Venafi</td>
<td>positive</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
</tr>
<tr>
<td>Vormetric</td>
<td>neutral</td>
<td>neutral</td>
<td>positive</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 18: Comparative overview of the ratings for vendors
It is possible in Table 13 to score a “critical” rating. In the area of Innovation, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in the analysis, integration with Certificate Management, Key Discovery, Tokenisation, and others. However, in this analysis all vendors scored at least neutral regarding this criterion.

The critical ratings are applied for Market Position in the case of vendors which have a very limited visibility (with that particular product and in general) outside of regional markets like France or Germany or even within these markets. Usually the number of existing customers is also limited in these cases.

In the area of Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base, but also based on some other criteria. This doesn’t imply that the vendor is in a critical financial situation; however the potential for massive investments for quick growth appears to be limited. On the other hand, it’s also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no or a very limited ecosystem with respect to numbers and regional presence. That might be company policy, to protect the own consulting and system integration business. However our strong believe is that growth and successful market entry of companies into a market segment relies on strong partnerships.

12.1 The Market/Product Matrix

Beyond that analysis, we have compared the position of vendors regarding combinations of our three major areas of analysis, i.e. market leadership, product leadership, and innovation leadership. That analysis provides additional information.
These comparisons for instance use the rating in Product Leadership on the horizontal axis and relate it with the rating in other areas, which is shown on the vertical axis. The result is split into four quadrants. The upper right quadrant contains products with strength both in the product rating and in the second rating we’ve looked at in the particular matrix, e.g. innovation. The lower right quadrant contains products that are overall strong but lack in the dimension shown on the vertical axis.

This for instance can be products that have strong technical capabilities but are relatively new to the market, resulting in a small customer base. The upper left quadrant contains products which are typically below average in the product rating but have specific strengths regarding the second dimension we look at in the particular matrix. They might be highly innovative or very mature and established, but not being leading edge when looking at the product rating. Finally, there is the lower left quadrant that contains products suffering on both axis. However, these products might have specific strengths that are highly valuable for some specific use cases.

In that comparison it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are over-performers when comparing Market Leadership and Product Leadership. It comes as no surprise that these are mainly the very large vendors, while vendors below the line frequently are innovative but focused on specific regions.

We have defined four segments of vendors to help in classifying them:

**Market Leaders:** This segment contains vendors which have a strong position in our categories of Product Leadership and Market Leadership. These vendors have an overall strong to excellent position in the market.

**Strong Potentials:** This segment includes vendors which have strong products, being ranked high in our Product Leadership evaluation. However, their market position is not as good. That might be caused by various reasons, like a regional focus of the vendors or the fact that they are niche vendors in that particular market segment.

**Market Performers:** Here we find vendors which have a stronger position in Market Leadership than in Product Leadership. Typically such vendors have a strong, established customer base due to other market segments they are active in.

**Specialists:** In that segment we typically find specialized vendors which have – in most cases – specific strengths but neither provide full coverage of all features which are common in the particular market segment nor count among the software vendors with overall very large portfolios.
12.2 The Product/Innovation Matrix

![Product/Innovation Matrix](image)

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with few exceptions. This distribution and correlation is typical for mature markets with a significant number of established vendors plus a number of smaller vendors.

We have defined four segments of vendors. These are:

**Technology Leaders:** This group contains vendors which have technologies which are strong regarding their existing functionality and which show a good degree of innovation.

**Establishment:** In that segment we typically find vendors which have a relatively good position in the market but don’t perform as strong when it comes to innovation. However, there are exceptions if vendors take a different path and focus on innovations which are not common in the market and thus do not count that strong for the Innovation Leadership rating.

**Innovators:** Here we find highly innovative vendors with a limited visibility in the market. It is always worth having a look at this segment because vendors therein might be a fit especially for specific customer requirements.

**Me-tooos:** This segment mainly contains those vendors which are following the market. There are exceptions in the case of vendors which take a fundamentally different approach to provide specialized point solutions. However, in most cases this is more about delivering what others have already created.
12.3 The Innovation/Market Matrix

![The Innovation/Market Matrix](image)

The third relation shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position.

On the other hand, vendors which are highly innovative have a good chance for improving their market position but might also fail, especially in the case of smaller vendors.

The four segments we have defined here are

**Big Ones:** These are market leading vendors with a good to strong position in Innovation Leadership. This segment mainly includes large software vendors.

**Top Sellers:** In that segment we find vendors which have an excellent market position compared to their ranking in the Innovation Leadership rating. That can be caused by a strong sales force or by selling to a specific community of “customer customers”, i.e. a loyal and powerful group of contacts in the customer organizations.

**Hidden Gems:** Here we find vendors which are more innovative than it would be expected when looking at their Market Leadership rating. These vendors have a strong potential for growth, however they also might fail in delivering on that potential. Nevertheless this group is always worth a look due to their specific position in the market.
Point Vendors: In that segment we find vendors which typically either have point solutions or which are targeting specific groups of customers like SMBs with solutions focused on these, but not necessarily covering all requirements of all types of customers and thus not being amongst the Innovation Leaders. These vendors might be attractive if their solution fits the specific customer requirements.

13 Mapping Products and Customer Requirements

When looking at EKCM solutions there are often some requirements that are more relevant for the client than others. For the benefit of easily being able to identify who are Leaders in some of these edge cases we have added the following diagrams focusing on:

- Certificate Management
- Key Management

![Figure 11: Enterprise Certificate Management Matrix](image)

This matrix shows that Venafi is still a clear leader in the Certificate Management area, although some of the larger HSM vendors fare relatively well, the point solution vendors are lagging behind due to their focus in the EKM space.
Conversely however, Venafi also score highly in the EKM matrix. The point solution vendors climbing higher due to their focus on key management applications rather than certificate management. SafeNet and RSA score more highly in the EKM space due to their Enterprise level solutions in this area.

## 14 Overall Leadership

Finally, we put together the three different ratings for Leadership, i.e. Market Leadership, Product Leadership, and Innovation Leadership and created an Overall Leadership rating. This is shown below in Figure 13.
There is a clear overall leader in Venafi, the only single Enterprise level, combined Key and Certificate management tool that covers multiple applications. Other products are close behind, particularly notable are Safenet and RSA who have complementary solutions to cover the both EKM and ECM, but not on one platform.

This is a complex area of constant change. Products are converging and developing at different rates in different areas. As always, leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. In this area, possibly more than others, a thorough evaluation of these requirements and a mapping to the features provided by the vendor’s products is mandatory.

Overall Leaders are (in alphabetical order):

- Safenet
- RSA
- Venafi

### 15 Vendors and Market Segments to watch

Besides the vendors covered in this KuppingerCole Leadership Compass on EKM, there are several other vendors which either declined participation in this KuppingerCole Leadership Compass, have only a slight overlap with the topic of this document, or are not (yet) mature enough to be considered in this document. This includes the following vendors which have key management solutions only:

**Hewlett-Packard**

HP’s Enterprise Secure Key Manager is geared up for key management related to ATM/POS solutions. A good performer in a niche space, but not an enterprise certificate management solution at this stage.

**Oracle Corporation**

Oracle Key Manager is another good key manager which operates in a niche, unsurprising perhaps for a company focusing on the security of their database offerings.

**Cryptomathic**

Software-based key manager with comprehensive lifecycle functions. Some good security features, including tamper-evident logs, and not restricted to a particular niche. A strong solution in the EKM space.

**Cisco Systems**

Storage media encryption only, an undeveloped point solution for use in SAN deployments. Fits with Cisco’s portfolio, but not a strategic enterprise tool.

**NetApp**

Point solution for NetApp storage sold out to SafeNet to be developed as their KeySecure manager. NetApp uses this as their solution. An interesting approach to key management development, decoupling it from the storage altogether and allowing a security company to develop it.
Quantum Secure

Disk and tape encryption only to support the Quantum product set. A niche solution set which would do well with a similar approach to that which NetApp has taken. A well-developed niche could be handed over to a security company for a better effect in the market.

Bell ID

Key management for EMV chip cards only. Smart card issuing systems require a large number of keys to be managed, this is one niche area where the key manager is of a sufficiently unusual usage that integration with certificate management or even the rest of the key management product set might not be of any significant advantage.

Symantec Encryption Management Server

The re-branding of PGP’s Universal Server as a Symantec product still needs some work to build out into a full key and certificate management solution. This may be why Symantec declined to take part in this LC at this time.

Voltage

Voltage have an interesting “stateless” solution which supports symmetric and asymmetric keys. They do not currently have a full certificate management solution, but would score highly amongst the key management solutions outlined here, particularly in terms of innovation.
Kuppinger Cole Ltd.
Am Schloßpark 129
65203 Wiesbaden | Germany

Kuppinger Cole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company Kuppinger Cole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

Kuppinger Cole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. Kuppinger Cole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact clients@kuppingercole.com