Mi-Token vs. Vasco vs. SafeNet vs. RSA vs. Entrust

Seed-file Security

Mi-Token

When soft-tokens are used, Mi-Token itself does not 'see' any of the seed files used by the soft-tokens at any stage. Instead, the token seed-files are encrypted end-to-end during the loading process in a specific node-to-node method – that is, only the Mi-Token backend servers (installed at the client side) and the soft-token itself ever sees the raw seed-file content. With hard-tokens of various kinds, Mi-Token supports on-customer-site reprogramming to again ensure the seed-files never leave the confines of the customer-site.

Mi-Token has full support for the use of Hardware Security Modules for additional security.

Mi-Token supports the encryption of seed-files in soft-tokens using 'deniable' encryption – that is, an offline attacker has no way of discovering if a potential decryption target is correct or not. No competing company offers this deniable encryption feature.

With Mi-Token, there is no possible point of attack external to your company's premises – and hence ultimately out of your control.

Vasco

Vasco typically generates seed-files for all clients for both hard- and soft-tokens of all types. In particular, should Vasco's seed-store or systems be compromised, then that could compromise soft-tokens that have not even been loaded yet. Vasco does not offer customer-side hard-token programmability.

Vasco does not support the use of Hardware Security Modules for additional security.

SafeNet

SafeNet, again, typically generates seed-files in advance – even for soft-tokens. This means that, as with Vasco, token seed-files can be compromised at a location outside of the customer site. Unlike Vasco, SafeNet at least allows – and encourages – soft-token seed-file generation at a customer site. However, their loading-mode constrains the entropy of the generated token-seed, slightly reducing security.

Unlike Vasco, SafeNet does allow on-site reprogramming of (some) hard-token types. The exact way SafeNet's seed security works differs across various products – after acquiring Aladdin, SafeNet has not had one unified product line.

SafeNet provides limited support for Hardware Security Modules.

RSA

RSA generates seed files in advance for all types of tokens. RSA's seed-file security has been compromised in the past and shows the vulnerabilities associated with their centralized database. RSA seed file transit is not secure, allowing attackers to intercept seed files. The seed file security issue has cost RSA customers a great deal of time and money to replace tokens and update systems. Hardware Security Modules

Entrust

Entrust IdentityGuard is a certificate based authentication system. It is harder to secure this type of system because mobile devices are directly tethered to the client's system, making a successful attack more likely especially if a phone is stolen.

IdentityGuard needs outbound access to the Internet to deploy tokens, which makes the files relatively easy to intercept.

Entrust IdentityGuard requires a dedicated server to store seed files and the authentication software, increasing the up-front cost drastically, as well as the time involved in deployment. The management of the system is labor intensive due to the required use of proprietary servers.

Token Enrolment

Mi-Token

Mi-Token allows for fully-automated, user-initiated soft-token creation and hard-token assignment, set within policy bounds as appropriate – perhaps users can assign themselves soft-tokens only within a certain timeframe. Users will always be required to enter credentials of some kind (e.g. username and existing static password) to assign themselves a soft-token. This is very customisable.

Mi-Token allows for some users to be assigned permission to vary a subset of other users – with these subsets completely individually configurable for each user. Mi-Token can quickly add or modify features in the soft-token provisioning site as required, to produce the exact process flow Bosch requires. These features can be created within a very short timeframe.

Mi-Token allows for users to load tokens without typing anything on their cell-phone, mobile device, or desktop application, but rather by only typing an 8-digit code on the provisioning site. Soft-Tokens can also be provisioned by sending an email to users, which automatically detects their device type and thence automates the loading process as much as possible.

The token loading process conveys no direct seed-file information in any information the user sends to the server. That is, the token and the customer site (via the Mi-Token site, which acts as a 'temporary encrypted record repository', communicate to each other the required seed information with end-to-end security. This means that an attacker cannot create an unnoticed duplicate of a token with information from the loading process – even in the worst case, an attack will be detected and the loading process will fail.

Mi-Token allows for the auto-assignment of a range of hard-tokens. This means that tokens can be mailed out to users en-masse without regard for token serial-numbers. This process can be regulated by appropriate security policies.

Vasco

Vasco provides limited self-provisioning options, all of which require significant administrator intervention. This is a very labour-intensive process.

During the enrolment process, information which is provided by the site that the user/admin enters into the token, and by the token that the user/admin enters into the site, provides all the information required to generate the seed-file used by the token. Thus, someone can make a perfect (undetected) duplicate of a token.

Vasco's provisioning system does not allow users to assign or manage tokens for other users.

The Vasco self-provisioning website is not customisable. Updates may be released in future, but at best, Bosch can slightly influence the contents of the next update – which will usually be months away!

SafeNet

SafeNet allows users to self-enrol, but even with their provisioning site, the process is typically long-winded and involves an administrator individually setting an enrolment passphrase for each user. There may be limited batch-assignment options available, but this probably involves emailing out (interceptable!) passphrases to users or the like.

During the enrolment process, information is provided by the site that the user/admin enters into the token, and by the token that the user/admin enters into the site, provides all the information required to generate the seed-file used by the token. Thus, someone can make a perfect (undetected) duplicate of a token.

The SafeNet self-provisioning website is not customisable. Updates may be released in future, but at best, Bosch can slightly influence the contents of the next update – which will usually be months away!

SafeNet's provisioning system does not allow users to assign or manage tokens for other users.

RSA

RSA charges for token enrolment, and requires the time and effort of administrators to handle the enrolment process. They do not offer self-deployment for end-user token enrolment. RSA does not have multiple options for token enrolment.

Bosch will not be able to take advantage of speedy updates with RSA, who set a certain number of update releases per year and cannot take on custom projects in the way that Mi-Token can.

Entrust

The enrolment of tokens is not secure due to the need for outward-facing Internet provisioning. The seed files can be intercepted much more easily in this solution. Entrust does offer end users access to their Self-Administration Server, but the functionalities and ease of use provided within that system are no match to the advanced self-administration features offered by Mi-Token.

Soft-Token Platforms

Mi-Token, SafeNet, Vasco, RSA, and Entrust have soft-tokens for all major platforms. Mi-Token offers Windows Phone 7 support, which is currently offered by SafeNet and is not explicitly supported by Vasco. All other major platforms (Blackberry, iOS, Android, Java-apps, etc.) are all supported. Mi-Token allows for unlimited free soft tokens per user on all platforms, whereas other solutions do not.

Hard-Token Options

Mi-Token

As Mi-Token is Token-Independent, Mi-Token supports any OATH-compliant token, covering a vast array of potential token choices. Furthermore, Mi-Token supports a broad range of proprietary tokens. These tokens include everything from bog-standard 6-digit OTP tokens to credit-card form factor tokens (including smart cards, RFID functionality and even completely functional credit cards!) to Yubikeys. Mi-Token allows for customers to buy their own tokens independently if they so desire. Mi-Token takes the view that tokens are commodities, allowing customers to very cheaply obtain hard-tokens.

Vasco

Vasco provides a small range of hard-tokens, including a single card-shaped token choice. Vasco only supports tokens sold by Vasco, locking customers in to buying expensive hard-tokens.

SafeNet

SafeNet supports a small range of hard-tokens, not including ‘credit-card’ form factors. SafeNet locks customers into using their small range of hard-tokens – as with Vasco – and has complete control over the pricing of their hard-tokens, allowing them to overcharge for them. SafeNet only supports tokens sold by SafeNet.

RSA

RSA offers hard tokens that expire after a set period of time, and require IT staff to manage enrolment of tokens, as well as keep track of the tokens in a required sequel database that takes up enormous processing power and time to manage. RSA tokens are costly, and customers are forced to use only RSA tokens through their lock-in business model.

Entrust

Entrust only supports their own hard tokens and forces customers into their proprietary lock-in model. Entrust is offering fewer and fewer options for hard tokens as they move away from providing hard token solutions to focusing on soft tokens. Choice for hard tokens is very limited, and their development efforts for hard tokens appear to be on hold.

Active Directory Integration

Mi-Token

Mi-Token does not touch the Active Directory schema, nor does it store any data in active-directory apart from a reference object pointing to the main Mi-Token instance – so it can be automatically located by administrative pieces and the like.

Mi-Token's UI integrates completely with the Active Directory Users and Computers snap-in, utilising familiar, intuitive administrative paradigms, allowing for very low management overhead; however, it shows up as an entirely separate area within the UI, keeping management tasks appropriately separated. This allows for Mi-Token administrative permissions to be set entirely independently of Active-Directory administrative permissions.

Mi-Token stores data in ADAM/ AD LDS databases, providing scalability and performance advantages without requiring the installation of complex SQL databases and the like.

Vasco

Vasco changes the Active Directory schema and stores a bevy of data in it. Vasco administration is directly integrated in with the AD UI, in such a fashion it is not always intuitive as to how to go about token-management operations. Furthermore, Vasco administrative permissions are not entirely independent of AD administrative permissions.

SafeNet

SafeNet changes the Active Directory schema and stores a bevy of data in it. Vasco administration is directly integrated in with the AD UI, in such a fashion it is not always intuitive as to how to go about token-management operations. Furthermore, SafeNet administrative permissions are not entirely independent of AD administrative permissions.

RSA

The administration for RSA is divorced from active directory, operating on a separate interface. The management of RSA is not intuitive, and takes a great deal of time to manage because of a required sequel database and a platform that makes token management inefficient.

Entrust

Entrust does not operate within active directory, but can integrate with systems that use Active Directory to store users. This process is cumbersome and does not integrate smoothly.

Customisability / Integration effort

Mi-Token

Mi-Token is a rapidly evolving and improving product, and customer requests are implemented quickly – typically within a month. Mi-Token has done a wide range of customisation work in the past across all areas of implementation – including the provisioning site. Mi-Token's API is trivially easy to integrate with, and new features are added to the API as they are implemented elsewhere.

Mi-Token can very quickly provide features or configuration changes upon request for demonstration, as Bosch requires them. Mi-Token will go to great lengths to reduce the amount of effort Bosch requires to implement this solution, as well as to provide the exact functionality required.

In the event of an error, Mi-Token can very quickly provide access to very high-level support – not just 'support engineers', but actual programmers! Mi-Token provides more than ample logging functionality, allowing for problems to be quickly diagnosed.

Vasco

Vasco's 2FA solution has not changed significantly over the last few years; feature requests take months – if not years – to be processed and their product is not very adaptable. Vasco's API efforts are complex; integration can take some time and usually involves significant effort on the customer side.

Troubleshooting can be quite frustrating and involves elevating cases through many levels of support.

SafeNet

SafeNet's 2FA solution range is a hodgepodge of solutions acquired at various points in time; different components do not always cooperate properly. As with Vasco, the product has not evolved much in the last few years; feature requests take many months to even be considered. If the implementation of a solution hits a hitch, significant effort at the customer side is usually required to fix it, with sparse help provided.

Troubleshooting can be quite frustrating and involves elevating cases through many levels of support.

RSA

RSA does not integrate well with most custom platforms because of its unnecessary complexity. The solution is out-dated and does not cover many current use cases required by customers. Updates take a long time to integrate, and requests for customization by customers are very difficult to implement. RSA does not integrate with many custom systems and sites because their proprietary lock-in model forces customers to use specific systems.

Entrust

Entrust does support some integration into custom applications, particularly in banking. They do not, however, have support for HSMs. The addition of functionality – either in terms of target language or supported operations – would take some time to move through Entrust's development cycle.