Comparison of Cloud-Based Signature Solutions and Cybernetica's SplitKey

White Paper

31.01.2020

8 pages

TABLE OF CONTENTS

Executive summary

The biggest difference between cloud-based signing solutions and SplitKey is that SplitKey can be used to offer secure authentication services as well as signing, whilst cloud-based signing solutions require an additional authentication technology in order to make the remote signing possible.

Why this is noteworthy is that any digital identity solution is only as secure as its weakest link, and with cloud-based offerings, the weakest link is the authentication technology. Different authentication solutions are used by cloud-based signing service providers that either require the distribution of hardware tokens (suitably secure, though inconvenient and costly) or rely on less advanced mobile offerings.

This gives SplitKey a significant advantage over cloud-based signing solutions, as SplitKey's authentication and signing functionality work in the same way, and use the same dedicated security hardware on the service provider's side as cloud-based offerings, but in a more advance, secure manner. SplitKey achieves a higher level of assurance with authentication and signing, while ensuring end-user ownership of their private keys, and reduced liability for the service provider in the event of an attack or breach.

1 Introduction

There are several PKI (public key infrastructure) digital signing technologies available on the market, with varying degrees of assurance. At the upper end of this scale, where government and financial institutions look for solutions, there are three kinds of technology that have been shown to achieve the right level of certification for private key protection, specifically, EAL4+. EAL4+, or evaluation assurance level 4+, is a Common Criteria evaluation. In short, it is cited as the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4+ for remote signing usually refers to hardware tokens with hardware protected keys, such as smart cards. The "+" represents an additional level of testing for resistance to high-attack-potential.

The three technologies at this end of the scale are hardware protected keys on chips (e.g. smart cards or SIM cards), cloud-based signing, and SplitKey. This white paper will focus on comparing the latter two solutions, which have gained popularity in recent years due to the ease of roll out and the convenience for the end-user; that is, cloud-based and SplitKey. There are several similarities between these two technologies, and when it comes to end-user experience, the difference can be unnoticeable, but where they do differ is around how the end-user's private keys and their use are protected on the client side, and the important aspects of ownership, responsibility, and trust.

1.1 Introduction to cloud-based solutions

In terms of PKI, cloud-based or remote signing solutions are characterized by managing and storing end-users' private keys in remote, centralised servers, protected by HSMs hosted by a service provider, often usable from any device or location. The act of signing using those private keys takes place on the service providers' HSMs, with permission to use the private keys being given by the end-user from their personal device in a number of possible ways.

Cloud-based signing solutions do not cover secure authentication as standard, and often leave this functionality up to the end-user or customer. Different tools that can be used include hardware-based options that store private keys on chips, or a wide range of smartphone-based options with varying degrees of security.

1.2 Introduction to SplitKey

SplitKey is characterized by generating and storing end-users' private keys in two shares on two separate devices; the service provider's server, protected by an HSM, and the end-user's smart device (tablet or phone). The key-share that is generated on the end-user's device is split into two individually unusable parts, one of which remains on the device, the other, sent to the server. What's left on the end-user's device is encrypted with a PIN code which isn't stored anywhere and known only by the end-user. The private key never exists in the whole - this is to say, it is generated as two shares, and neither during registration, nor authentication and signing (or at any time), do these shares get combined.

The act of authentication or signing using the private keys is an interactive process, with the signature being created in parts; one on the end-user's device using the private key-part stored there, and two on the HSM with the other two key-parts the HSM protects. The signature-parts are combined on the service provider's HSM to create the full signature for either authentication or digital signatures.

2 Main comparative differences

SplitKey is not unlike cloud-based solutions in that a service provider's HSM is used to protect private keys, and the final act of applying the end-user's signature takes place on this HSM. How this stage of signing is reached and controlled though, is the key to how these technologies differ, both on the client side and service provider's side.

2.1 Client side

The greatest difference between these two kinds of technologies is what part the end-user and their device plays. With cloud-based solutions, there is effectively no "client side", as the end-user is never in possession of their private key; the specific component in PKI that gives end-users the high assurance method of identifying themselves. As mentioned above, cloud-based solutions only function on the service provider's servers and rely on an additional technology or service in order to authenticate and provide permission for signing. In place of the traditional PKI methodology, where it is assumed the end-user is in possession of their private keys, end-users use a device that gives permission to the service provider to authenticate and sign on their behalf, as the end-user device does not contain any cryptographic signing material related to the keys on the server. There are two reasons often quoted for this; the first being the ability to give signing permission remotely, from any device, as the private keys are stored centrally. The second reason is that the end-user devices are not considered secure enough to protect private keys, though it must be noted, the end-user device becomes the proxy for protecting the use of the private keys held on the server.

The equivalent client side, or application side, of cloud-based solutions can vary in how permission is given and what security and layers of defence are used to ensure that only the end-user has the ability to provide this permission. The act of giving permission and the act of signing are effectively independent, meaning there is a need to rely heavily on the security of the permission giving device, which varies greatly across types of devices, age of devices, brands, and models. Any scenario where the permission/authentication solution is as strong or stronger than the signing solution deems the signing technology redundant.

With SplitKey, the end-user possesses a part of their private key on a smart device, enforcing ownership of the keys technically, as opposed to in cloud-based solutions, where control is enforced procedurally. They also have the ability to have multiple devices each storing a private key-part related to the same digital identity. Possessing this part of the private key means nothing can happen server side without input from the end-user's device. Going one step further, as the private key-part is encrypted with a PIN code that's not stored anywhere, the key-part on the end-user's device is useless without input from the end-user and cooperation from the server.

The PIN code used by the end-user to decrypt their private key-parts for authenticating or signing can only be verified once the signature-part created on the end-user device is combined with its equivalent signature-part on the host's HSM. This means, online or offline brute forcing is impossible. As the PIN code is not present on the device, and the key-part on the end-user's device is truly unusable in this form, no amount of time or computing power with the device alone would lead to an attacker being able to act on behalf of the user. This is true no matter the make or model of smart device.

2.2 Host side

As mentioned above, with cloud-based solutions, the end-users' private keys are stored in their entirety in the server of the service provider, protected by their HSM. This puts 100% of

the responsibility in the service provider's hands, and leaves them fully liable in the event of a breach or leak. Though there is little question HSMs are highly effective at protecting private keys from outsider attackers, the same cannot be said for an insider attack, and 34% of attacks involve an insider. Though human error or an attack leading to the loss of private keys is rare, possession of the private key plays a strong role in building trust, as end-users are used to knowing their identity documents and private keys cannot be used without their knowledge as long as they are in possession of them, which is the case with passports, smart cards, SIM cards, and other traditional and hardware-based solutions.

With SplitKey, though some of the end-user's private key is protected by the service provider's HSM, possessing a vital part of that key ensures the end-user is genuinely in control. As long as the end-user is in possession of the smart device which stores their private key-part, it is all but impossible for anyone to act on their behalf. Furthermore, not storing entire private keys in a centralized database ensures that any attack on the system can only ever be a 1-by-1 attack, as a large-scale attack would require interaction with each individual end-user in addition to the service provider in order to obtain and decrypt private keys. This means reduced risk for the service provider in terms of liability in the event of a breach or data leak.

3 Comparison table

	SplitKey	**Cloud Signatures**
No additional hardware on client side	X	Depends
Telco independent	X	X
Works with mobile	X	X
EAL4+ compliant	X	X
User possesses their key or part there of	X	
Auth and sign at same security level	X	
Includes secure authentication as standard	X	
Resistant to SIM hacking	X	X
Decryption of key doesn’t happen offline	X	x
Is not susceptible to server-side attack	X	
Does not rely on phone security (excl. OS) to protect key	X	Depends

4 Conclusion

It can be difficult to compare SplitKey with cloud-based signing solutions, as cloud-based solutions do not have secure authentication functionality as standard. Cloud-based solutions rely entirely on the service provider's HSMs to protect the end-user's private keys, and then rely entirely on a separate technology to protect the use of these keys. SplitKey shares the responsibility of protecting and using the private keys between the end-user and dedicated security hardware.

Digital identity solutions are built on trust as much as they are on technology, and enabling the end-user to possess what is truly used to identify them helps to build that trust. When the end-user has ownership of their private keys, there is a reduced need to place their trust in the service provider.

Aside from cloud-based solutions having increased liability on the service provider's side due to centrally stored private keys, the ability to enable true end-user ownership with the same level of protection as hardware-based technologies is what makes SplitKey a very suitable upgrade technology from token based digital identity services that use things like smart cards or SIM cards. It is through security and ownership by design that SplitKey can offer end-users true possession of what they use to identify themselves as part of a mobile solution, which has, so far, not been achieved in any other way.