Digital timestamps

Kangaroos Team

APPSEC

06.04.2014

Po co?

Time Stamp Authority

The TSA is a TTP (Trusted Third Party) that creates time-stamp tokens in order to indicate that a datum existed at a particular point in time

Możliwe zastosowania

- verify that a digital signature was applied to a message before the corresponding certificate was revoked thus allowing a revoked public key certificate to be used for verifying signatures created prior to the time of revocation
- indicate the time of submission when a deadline is critical
- indicate the time of transaction for entries in a log

Wybrane wymagania co do TSA

1. to use a trustworthy source of time.
2. to include a trustworthy time value for each time-stamp token.
3. to include within each time-stamp token an identifier to uniquely indicate the security policy under which the token was created.
4. to only time-stamp a hash representation of the datu
5. not to examine the imprint being time-stamped in any way (other than to check its length, as specified in the previous bullet).
6. not to include any identification of the requesting entity in the time-stamp tokens.
7. to sign each time-stamp token using a key generated exclusively for this purpose and have this property of the key indicated on the corresponding certificate.

O kluczu prywatnym

The certificate corresponding to the private key MUST contain only one instance of the extended key usage field extension as defined in [RFC2459] Section 4.2.1.13 with KeyPurposeID having value: **id-kp-timeStamping**. This extension MUST be critical.

Bezpieczeństwo

When a TSA shall not be used anymore, but the TSA private key has not been compromised, the authority's certificate SHALL be revoked.
reasonCode (CRL extensions):

- unspecified (0)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)

In that case, at any future time, the tokens signed with the corresponding key will be considered as invalid, but tokens generated before the revocation time will remain valid.
When the reasonCode extension relative to the revoked certificate from the TSA is not present in the CRL entry extensions, then all the tokens that have been signed with the corresponding key SHALL be considered as invalid.

Bezpieczeństwo

When the TSA private key has been compromised, then the corresponding certificate SHALL be revoked.

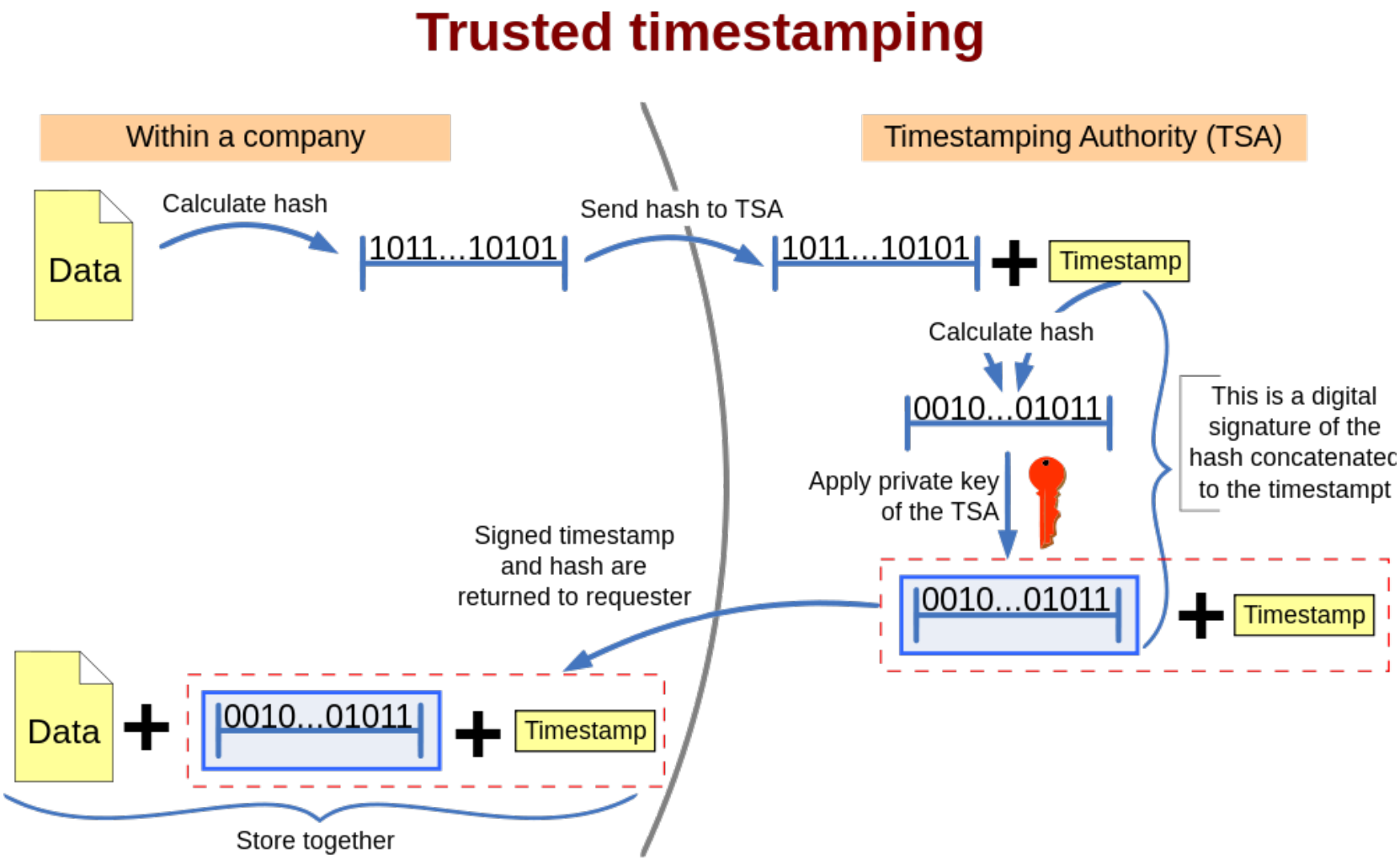
- reasonCode: keyCompromise (1) or extension not present

Any token signed by the TSA using that private key cannot be trusted anymore. In case the private key does become compromised, an audit trail of all tokens generated by the TSA MAY provide a means to discriminate between genuine and false backdated tokens. Two time-stamp tokens from two different TSAs is another way to address this issue.

Bezpieczeństwo

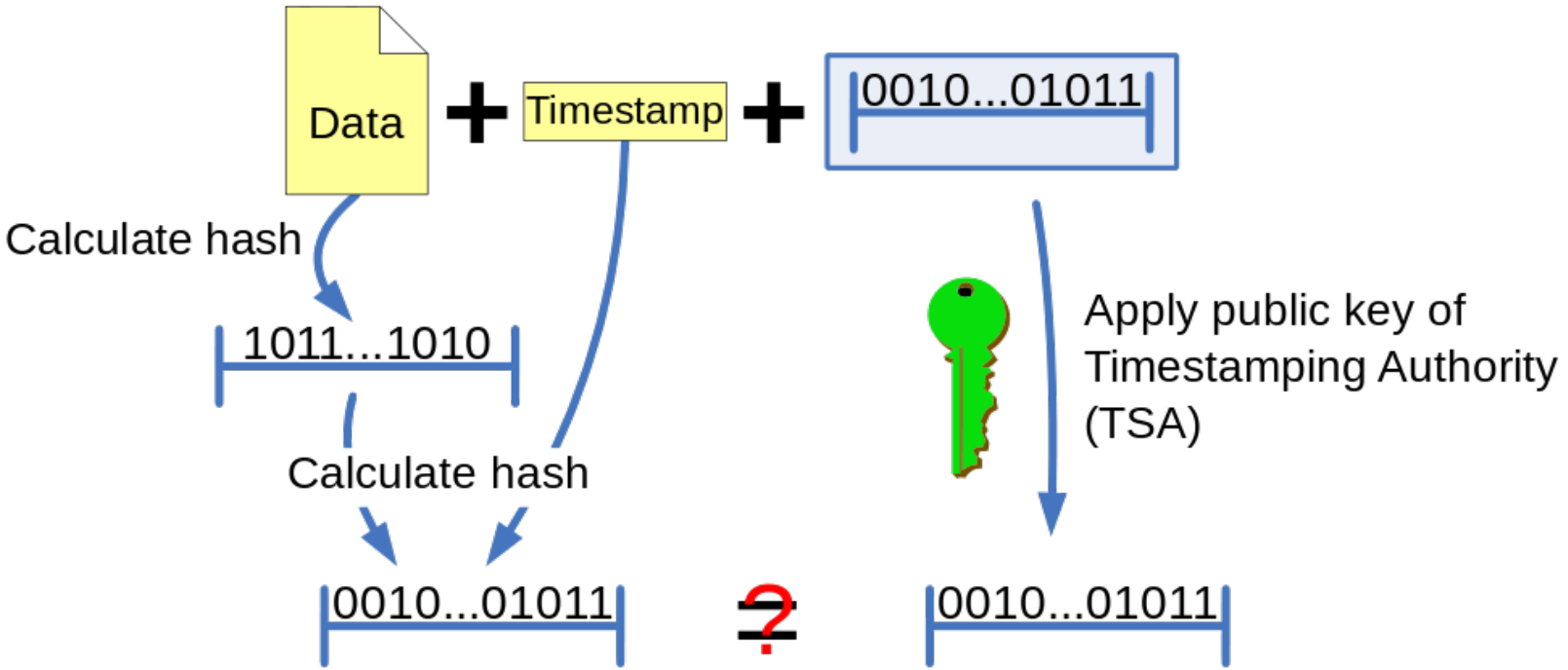
The TSA signing key MUST be of a sufficient length to allow for a sufficiently long lifetime. Even if this is done, the key will have a finite lifetime.
sThus, any token signed by the TSA SHOULD be time-stamped again (if authentic copies of old CRLs are available) or notarized (if they aren't) at a later date to renew the trust that exists in the TSA's signature. time-stamp tokens could also be kept with an Evidence Recording Authority to maintain this trust.

Zdobywanie timestampa



Weryfikacja timestampa

Checking the trusted timestamp



If the calculated hashcode equals the result of the decrypted signature, neither the document or the timestamp was changed and the timestamp was issued by the TTP. If not, either of the previous statements is not true.