

Digitala signaturer i praktiken



Det första svenska företaget att erbjuda ett säkert signatursystem enl. 8 § lagen om kvalificerade signaturer (2000:832).

Kvalificerade signaturer

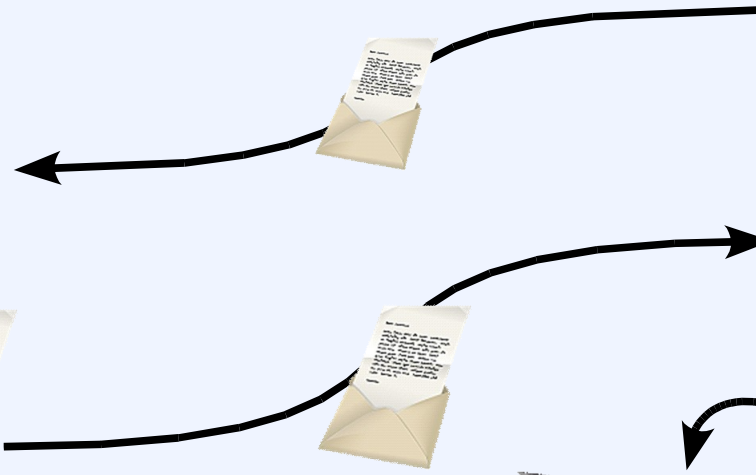
- Europeisk standard
- Säkert framställd
- Vi kan alltid entydigt kontrollera innehavaren
- Verifiering kostnadsfri för slutanvändaren
- Ersätter den handskrivna namnteckningen

SignGuard Europe AB

- Erbjuder:
 - Kvalificerade certifikat
 - OfficeSigner
 - Signeringsmjukvara för den enskilda arbetsplatsen
 - AutoVerifier & AutoSigner
 - Serverbaserade mjukvaror för verifiering & signering
 - HashSafe
 - Mjukvara för att säkerställa en bevisframställning av digitalt signerade dokument i framtiden

För 100 år sedan?

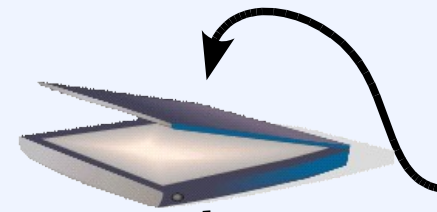
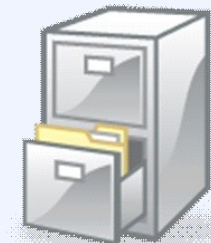
Axel i Hannover



Simon i Stockholm



Arkiv



- Tid: En vecka
- Total portokostnad: ca 100 kr
- Hur vara säker på vem som skrev under?

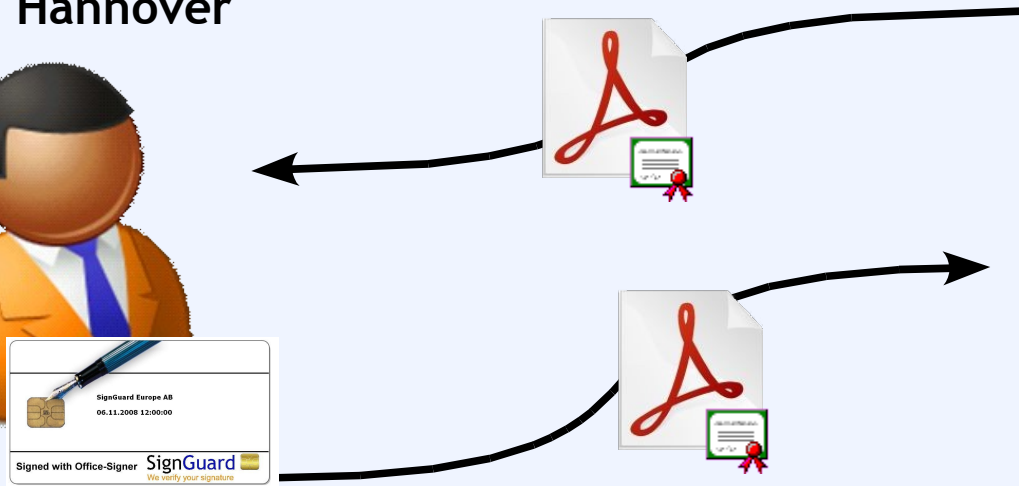
Idag

Axel i Hannover



Simon i Stockholm

Arkiv

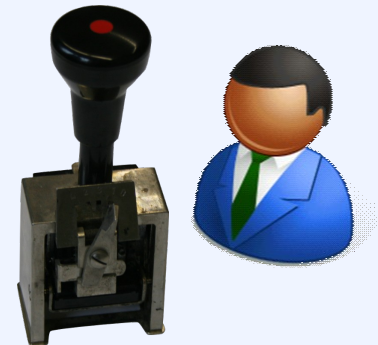


- Tid: mindre än en timma
- Portokostnad: ingen
- Lätt att arkivera dokumentet digitalt
- Enkelt att verifiera - dessutom kostnadsfritt

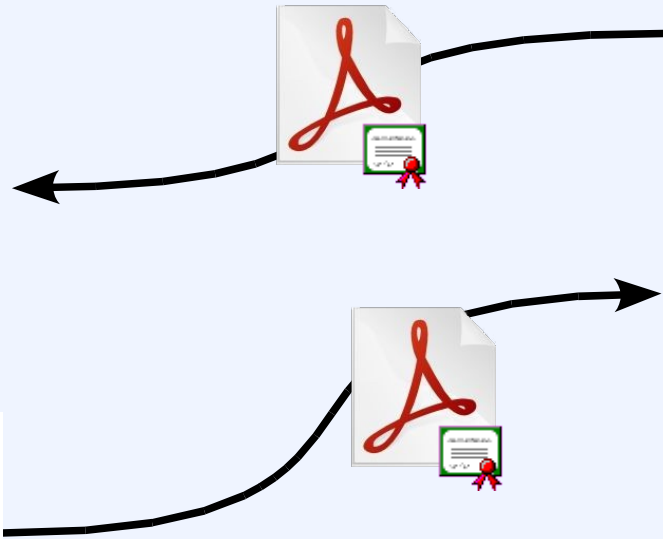
Digitala stämplor: Användningsfall

Organisation i Frankfurt

// **SkandicInkasso**



Peter



AutoVerifier

- SignGuards AutoVerifier verifierar signaturer automatiskt
 - Kostnadsfri användning genom SignGuard.se
 - Mer än 10 utgivare av kvalificerade certifikat inom EU som följer EG-direktivet 1999/93/EG
 - Dessa utgivare når idag en befolkningsmängd på mer än 120 miljoner individer
 - AutoVerifier kan verifiera signaturer från alla dessa!

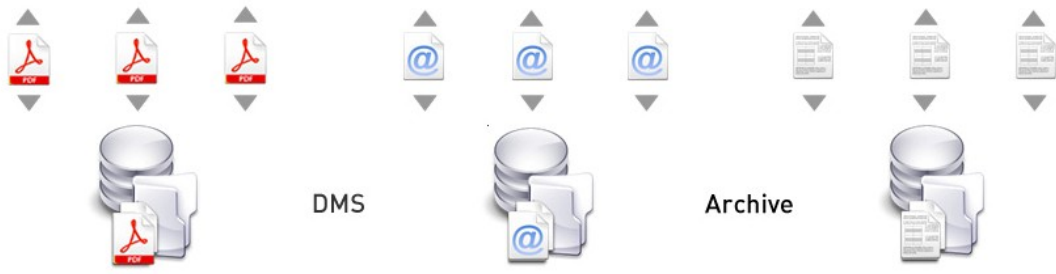
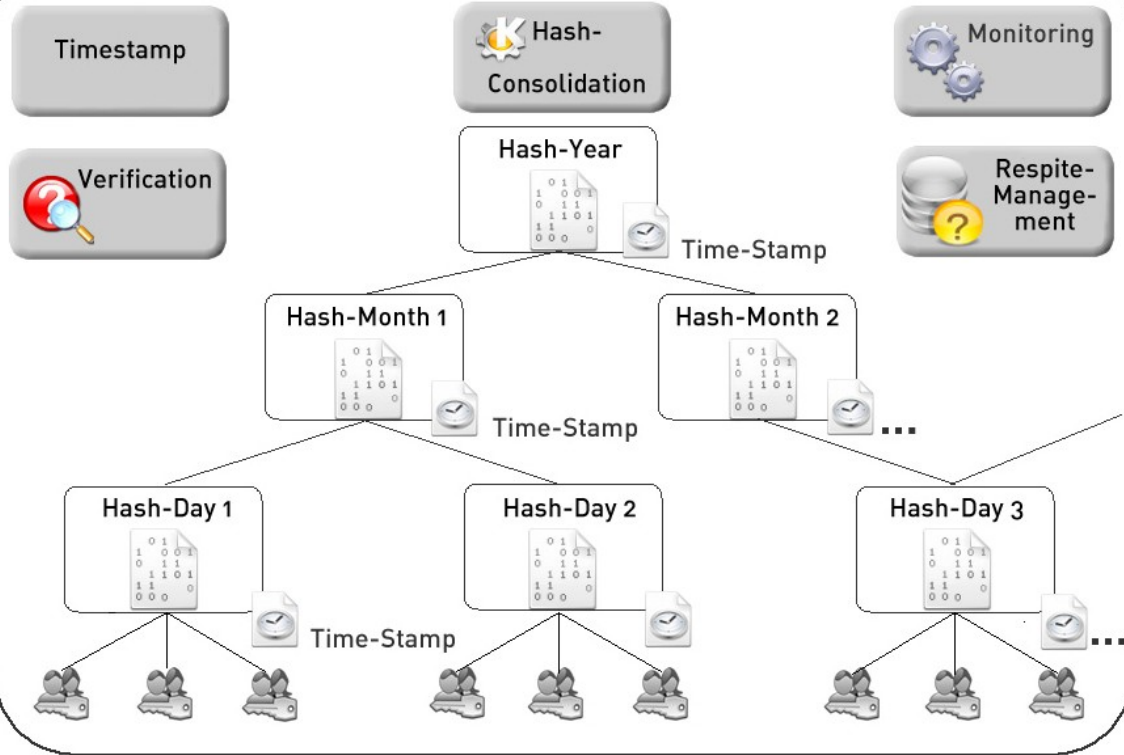
HashSafe: Motivation

- Qualified signatures are based on cryptographic algorithms:
 - Digest algorithm to produce a unique fingerprint (hash value) for a document
 - Encryption algorithm to encrypt the hash value
- Problem: Integrity of the signature is uncertain if an algorithm used is cracked or has an insufficient security suitability
- Consequence: Evidence value of qualified electronic signature is irreparably lost!

Solution: HashSafe

- To preserve the evidence value stronger cryptographic algorithms with security suitability are used
- System for long-term archival for signatures complies with ArchiSafe, LTANS:ERS (ISO):
 - Signature / Hashtree archive
 - Connector to (document) archive
 - Timestamping service connector
 - Monitoring service
 - Signature verification

Hash-Safe long-term Signaturearchive



Verification software

- HashSafe can be monitored and operated using a software from the HashSafe package
- Functions:
 - Export of an evidence record according to RFC 4998 (ERS):
 - Presentation of a specific document
 - Browsing through the available data
 - Start a manual check of signature validity for a predefined period of time
 - Adapting the policies for verification