alpin

Signatur & digitale Identität (SPID) - die nächsten Digitalisierungs-treiber?

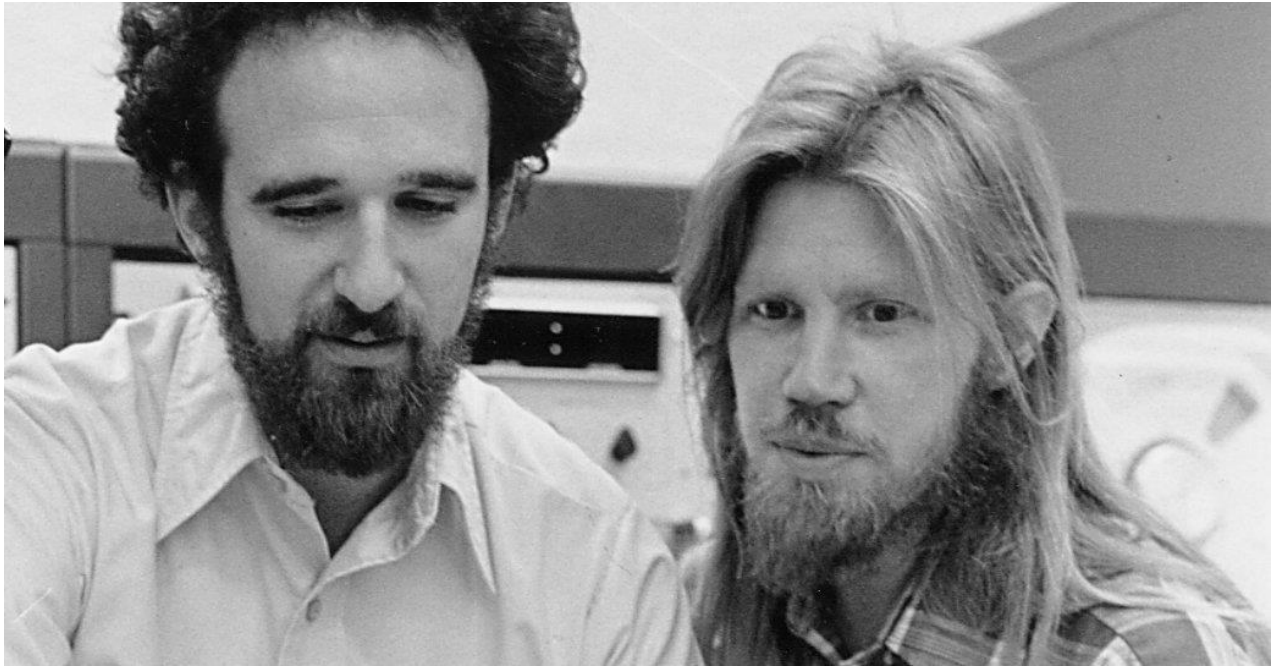
streamline your business

1.

Die Ursprünge der Digitalen Signatur.

Historische Grundlagen.

alpin



Martin Hellman and Whitfield Diffie in 1977

alpin

"

1976 stellten sich Whitfield Diffie und Martin Hellman eine Zukunft vor, in der Menschen regelmäßig über elektronische Netzwerke kommunizieren und anfällig dafür sind, dass ihre Kommunikation gestohlen oder verändert wird...

1976

alpin

"

1977 bauten darauf Ronald Rivest, Adi Shamir und Leonard Adleman den RSA Algorithmus, der dazu verwendet werden konnte, digitale Signaturen zu erstellen.

1976 1977

alpin

"

1989 lancierte die erste verbreitete Software, die den RSA Algorithmus kommerziell einsetzte, Lotus Notes 1.0.

1976 1977 1989

Diffie & Hellmann erhalten 40 Jahre später den Turing Award, die höchste Auszeichnung im Wissenschaftsfeld der Informatik.

1976 → 1977 → 1989 → 2016

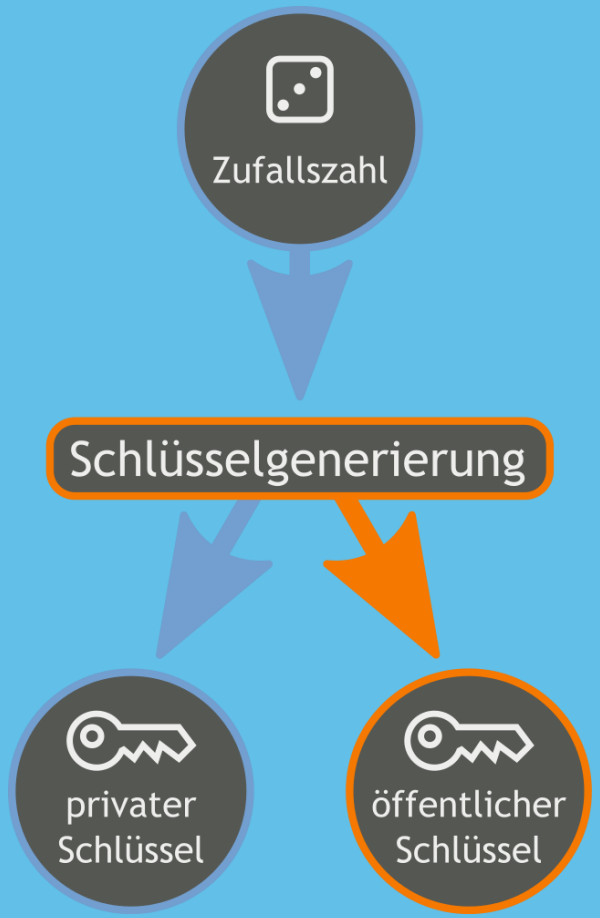
alpin

2.

Die Funktionsweise der Digitalen Signatur.

Mathematische Grundlagen.

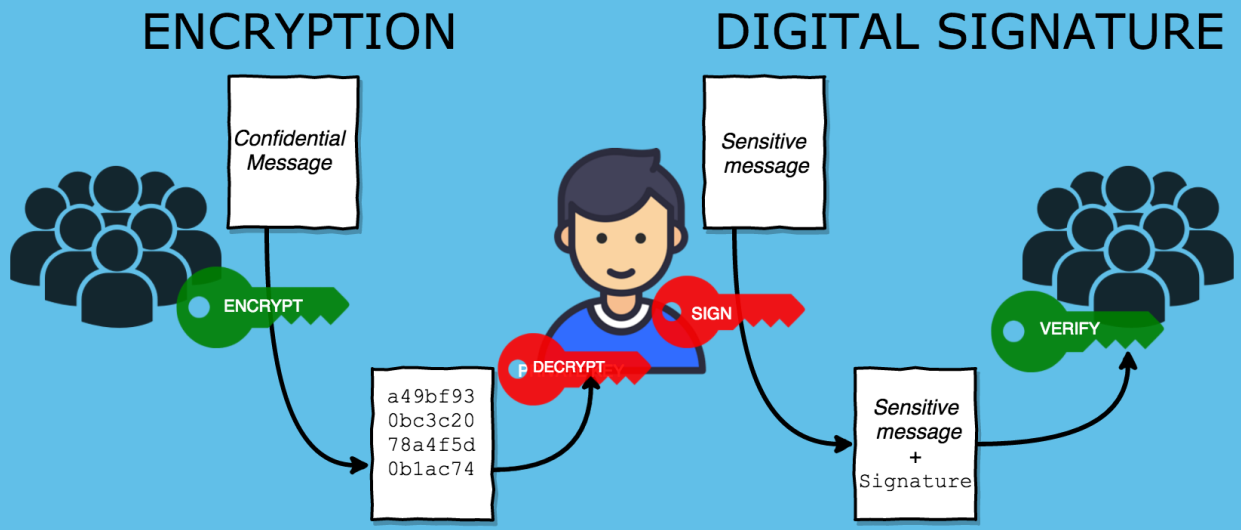
streamline your business



alpin

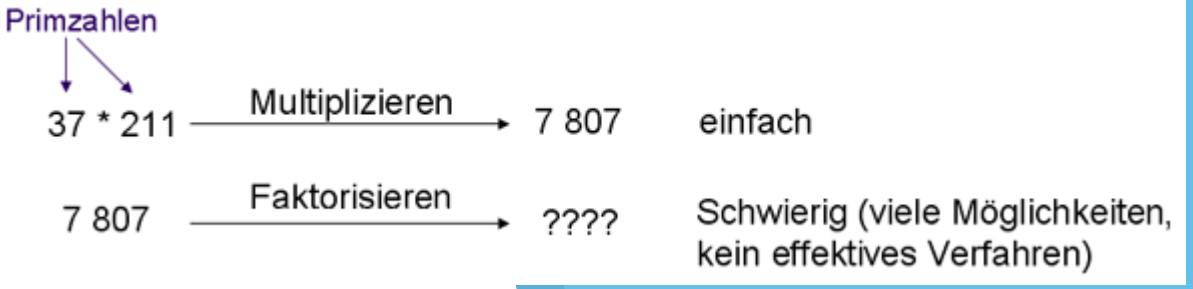
streamline your business

alpin



streamline your business

Einwegfunktionen



alpin

Die größten Rätsel der Mathematik!

P = NP ?

streamline your business


alpin
streamline your business

3.

Die Einführung in Italien und EU.

Anwendungen
im
Geschäftsleben.

streamline your business

Rechtlicher Rahmen und Einführung.

- Beginnt mit der Richtlinie 1999/93/EG, Richtlinie des Europäischen Parlaments und des Rates über einen Gemeinschaftsrahmen für elektronische Signaturen;
- Die am 19. Januar 2000 im Amtsblatt der Europäischen Union veröffentlichte Nr. 13 trat am 19. Januar 2000 in Kraft;
- Italien hat die Richtlinie 2002 (Gesetzesdekret Nr. 10 vom 23. Januar 2002) übernommen und heute mit dem digitalen Verwaltungscode angepasst;

Codice Amministrazione Digitale.

- Das heutige Gesetz über die elektronischen Signaturen ist das „Codice Amministrazione Digitale" (Gesetzesdekret Nr. 82 vom 7. März 2005), das im Laufe der Zeit verschiedene Änderungen erfahren hat;
- zuletzt durch Gesetzesdekret Nr. 179 vom 18. Oktober 2012;
- ergänzt durch das Gesetz „legge di conversione“ Nr. 221 vom 17. Dezember 2012).

eIDAS Verordnung der EU.

- eIDAS (englisch electronic IDentification, Authentication and trust Services), in Deutschland auch IVT, bezeichnet die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt;
- und zur Aufhebung der Richtlinie 1999/93/EG (Signaturrichtlinie).

Einführung der digitalen Signatur in Italien.

- Nationale Umsetzung der EU Richtlinie 2002;
- Digitale Signatur von zu hinterlegenden Bilanzen (Telemaco, 2003 und ff.);
- Zwingend für alle Vorgänge mit dem registro imprese ab 01.11.2003;
- Einführung der CNS carta nazionale servizi 2004;
- Signaturlösung d3sign.italian bereits 2005 von Alpin realisiert, Partnerschaft mit Actalis für Zertifizierungsdienste.

4.

Pitfalls?

Die Schwierigkeiten im täglichen Leben.

streamline your business

alpin

2FA (two-factor authentification)

streamline your business


alpin
2007 !
streamline your business


Carta Nazionale dei Servizi
CARTA REGIONALE dei SERVIZI
REPUBBLICA ITALIANA
TESSERA SANITARIA
CARTA REGIONALE DEI SERVIZI
Codice Fiscale RSSMRO62B25E205Y
Sesso M
Cognome ROSSI
Nome MARIO
Luogo di nascita CASSINA DE' PECCHI
Provincia MI
Data di nascita 25/02/1962
Data di scadenza 10/10/2019
RegioneLombardia


Carta Nazionale dei Servizi
delle CAMERE DI COMMERCIO D'ITALIA
Carta Nazionale dei Servizi
Camera di Commercio
Camera di Commercio Industria Artigianato e Agricoltura
Camera di Commercio
Carta Nazionale dei Servizi

2003 !

alpin

"

- ✓ Installation Pkcs#11 CSP Treiber
- ✓ Installation Lesegerät Treiber
- ✓ Multivendor Treiberkit bit4id
- ✓ Ergebnis: Unterschreiben am eigenen PC.

- aber Unterschreiben am fremden PC?
- und mobiles Unterschreiben?
- und USB Sticks? Eine Verschlimmbesserung!
- Und EU weite Interoperabilität? Theorie eIDAS 01.07.2016 vs. Praxis..


alpin
streamline your business

5.

Ubiquität & no hardware!

Firma remota.

streamline your business

alpin

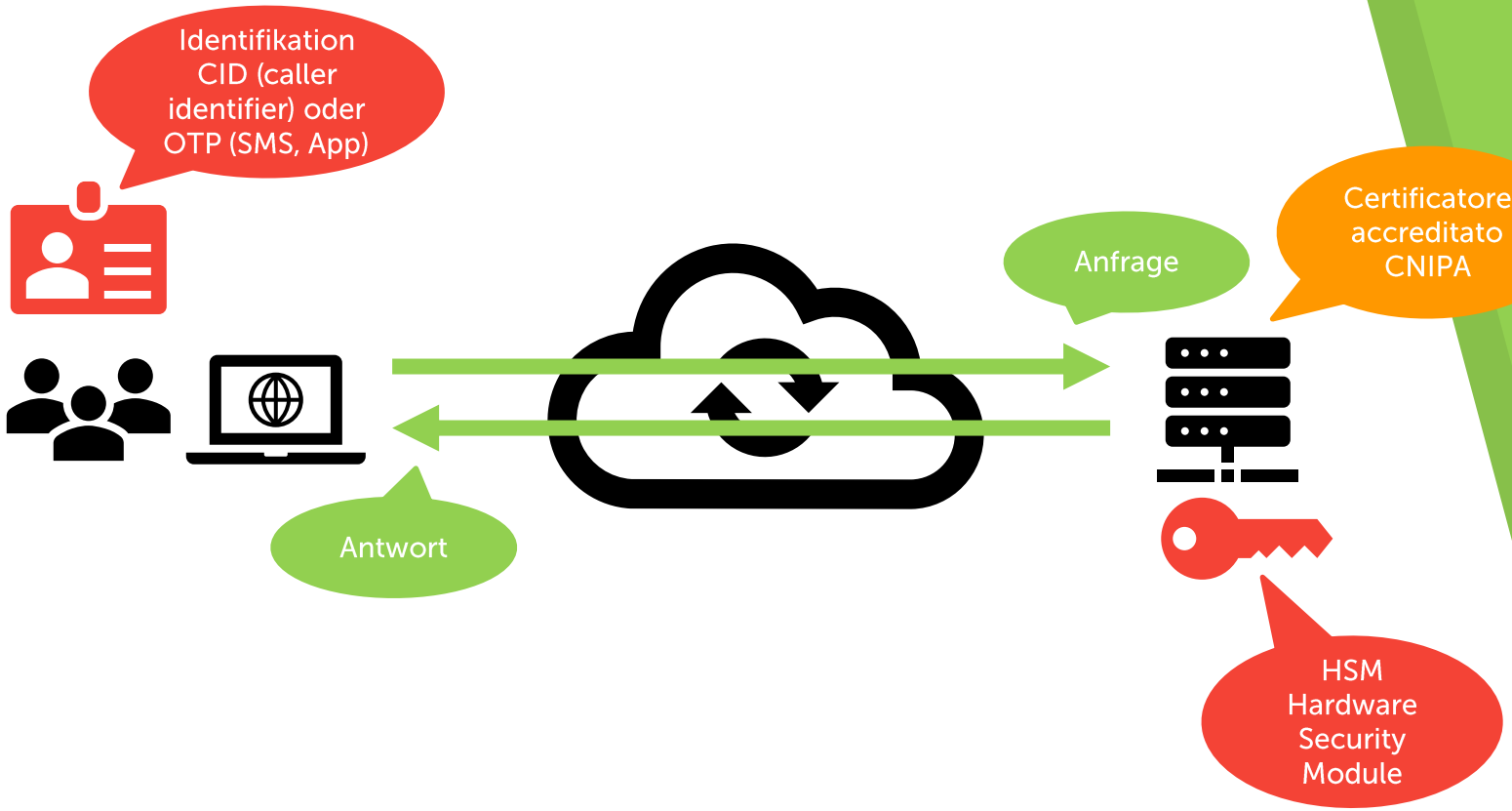
Quando gli utenti sono molto numerosi (da migliaia fino a milioni di utenti) ed operano in ambienti eterogenei, gli strumenti tradizionali di firma digitale possono rivelarsi problematici, oltre che eccessivamente costosi.

2008, Adobe, Actalis, AndXOr

Smart-card

Token USB

Firma
Digitale Remota


Identifikation
CID (caller
identifier) oder
OTP (SMS, App)
Anfrage
Certificatore
accreditato
CNIPA
Antwort
HSM
Hardware
Security
Module

alpin

Vorteile

- Keine Hardware
- Keine Treiberinstallation
- Unkompliziert
- Mobile Nutzung
- Breite Anwendungsszenarien

alpin

Facts

- Von 5 Personen in 2008 ausgedacht
- 2017 bereits 1.876.379.223 remote Signaturen erstellt

alpin

Nachteile?

Ist SMS wirklich eine 2FA?

2019 – das Jahr der SIM Swap/SIM Port Attacken!

Typical Online Identity

The configuration of a typical online identity.

alpin

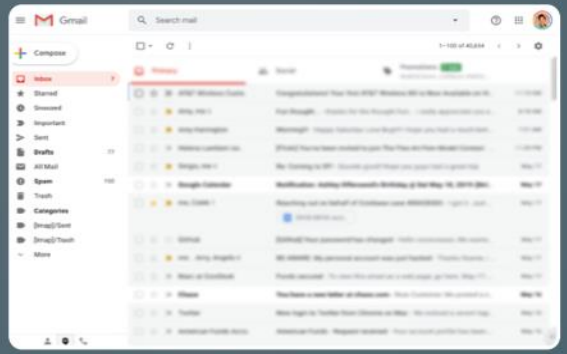
You

Your Mobile Device

SIM Card

Your SIM card binds your your phone number to your mobile device.

Your Primary Email Account



2FA Recovery Flow

1. If you forget the password to your email account, you can request a verification code be sent to your mobile device.

2. This code is then used to recover your account.

3. Your primary email address is connected to **a lot** of other online services.

etc.

streamline your business


alpin
streamline your business

alpin

Und jetzt?

- Hausaufgabe für die Telefongesellschaften.
- Die Kritizität der eigenen SIM verstehen.
- Wo möglich, 2FA über fido/U2F nutzen.
- Wo möglich, Auth Apps (Google Authenticator, Authy etc.) nutzen.

alpin


alpin
Esc
F1
~
`
!
1
streamline your business


alpin
No SIM
Cancel
12:19 PM
Multi-factor required
yubico
Ready to Scan
Verify login by touching your Yubikey to the top left of your mobile device.
Cancel
streamline your business

alpin

6.

SPID?

Sistema Pubblico di Identità Digitale.

streamline your business

alpin

"

Beginn der Arbeiten in 03/2013

Normierung über DPCM 24/10/2014

Reglements in determinazione AGID 28/07/2015

Livegang 12/2015 (InfoCert, Poste, TIM)

Livegang 09/2016 (Aruba, Sielte)

Livegang 05/2017 (Namirial, Register.it)

Federation über SAML 2.0 Standard

Welcome to eIDAS, welcome to Europe

alpin

AGID | Agenzia per l'Italia Digitale

alpin

"

Next Ideas?

- 27.01.2018 Codice Amministrazione Digitale
- Ein «documento informatico» kann «previa identificazione informatica del suo autore» erstellt (formato) werden.
- Es wird dabei ausdrücklich an SPID gedacht.

  Für die Umsetzung wartet man «Linee Guida AgID» ab.

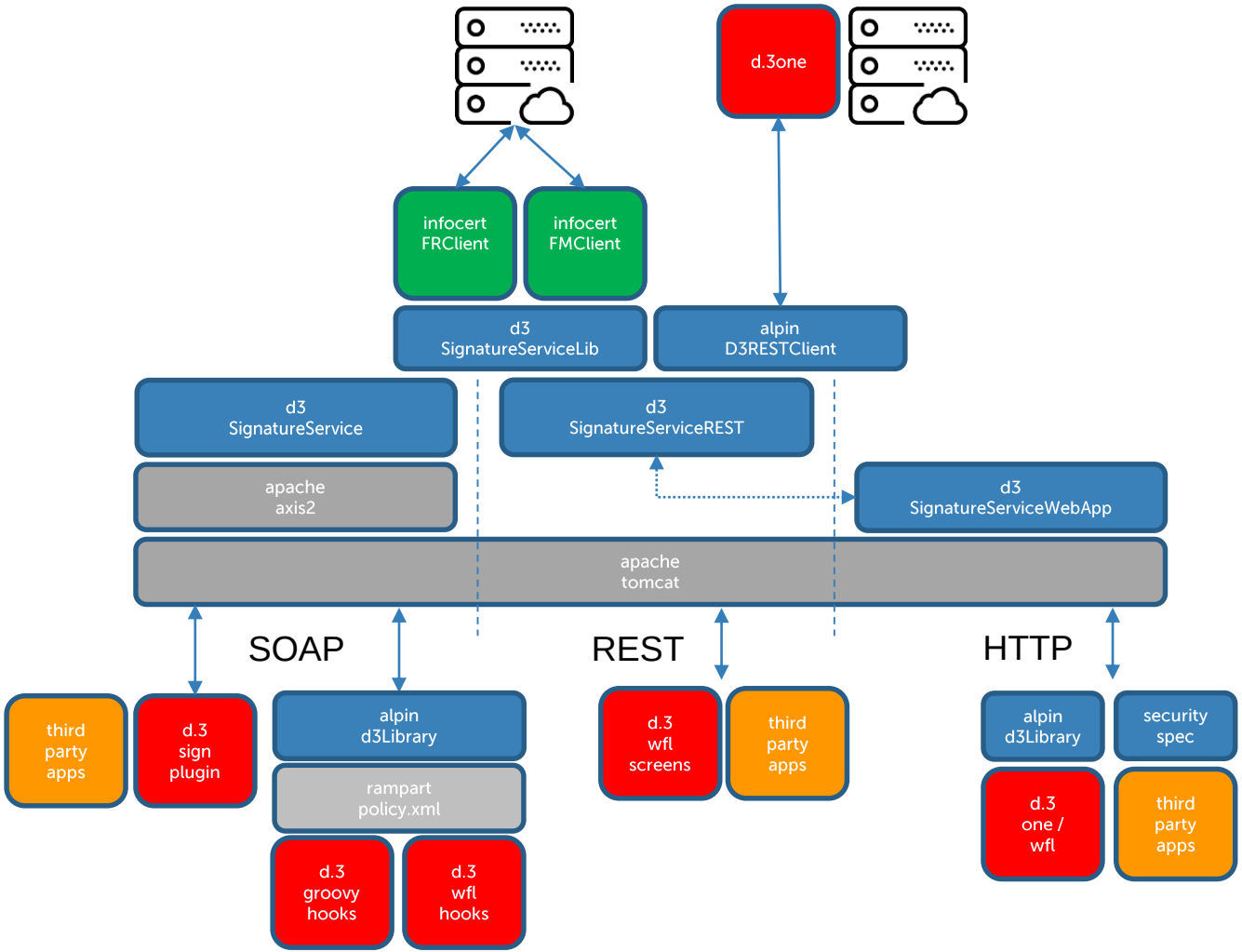
  SPID kann das Werkzeug für die Authentifizierung werden, mit der dann auch der Bürger digitale Dokumente unterzeichnen kann.

7.

Infrastruktur
d3Signature Webservices

Ziele

- Bereitstellung von remote signature Operationen
- Kapselung und damit Austauschbarkeit der dahinterliegenden Anbieter (InfoCert, Aruba, ...)
- Nutzung innerhalb von d.3 oder in Drittsystemen
- Bereitstellung unterschiedlicher technologischer Zugänge (API, SOAP, REST, WebClient)
- Ergebnis: eine einfache! Nutzung von digitalen Signaturoperationen dort, wo das Dokument entsteht oder verarbeitet wird.


d.3one
infocert FRClient
infocert FMClient
d3 SignatureServiceLib
alpin D3RESTClient
d3 SignatureService
d3 SignatureServiceREST
apache axis2
d3 SignatureServiceWebApp
apache tomcat
SOAP
REST
HTTP
third party apps
d.3 sign plugin
alpin d3Library
rampart policy.xml
d.3 groovy hooks
d.3 wfl hooks
d.3 wfl screens
third party apps
alpin d3Library
security spec
d.3 one / wfl
third party apps

8.

Chancen?

Disruptiv.


alpin
streamline your business

alpin

"

In der Planwirtschaft hatte Estland an Bedarf und Ressourcen vorbei aufgebaut.

1991 wurde Estland unabhängig, und hatte 1993 noch zum Beispiel ein Telefonsystem von 1938!

- Aus Helsinki kam damals das Angebot deren altes, analoges System zu übernehmen.
- “Wir wollen nicht in Technologien von 1979 hängen bleiben”, so damals Toomas Hendrik Ilves, später Präsident von Estland von 2006 bis 2016.
- Seit 2013 sind 95% der Fläche Estlands mit 4G LTE-Netzen abgedeckt.

alpin

"

- Ilves stößt ab 1996 die Programme Progetiiger und Tiigrihüpe an, mit dem Ziel, das Land großflächig mit moderner Computer- und Netzwerkinfrastruktur auszustatten und Programmieren bereits den Grundschülern beizubringen.
- In den 2000er Jahren haben die Esten vieles davon umgesetzt, was bsp. Deutschland heute noch erst diskutiert.

alpin

"

- mehr als 600 E-Government-Dienste, von der elektronischen Steuererklärung bis hin zum E-Voting
- die einzigen drei Gründe, warum man in Estland überhaupt noch ein Amt von innen sehen muss sind Heirat, Scheidung und der Kauf eines Hauses
- mehr als 99 Prozent der 2400 Staatsservices funktionieren online
- X-road, mehr als 900 verbundene Netze und Systeme
- eine zentrale Datenbank sorgt für aktuelle Bürgerdaten, auf die die Öffentliche Hand und die Unternehmen zugreifen können;
- Bereits Ende 2013 hatten die 1,3 Millionen Esten insgesamt 130 Millionen Mal im Netz elektronisch unterschrieben.
- 2017 waren es schon mehr als 500 Millionen Transaktionen pro Jahr.

Die wesentlichen Treiber?

Verbot für die öffentliche Hand, Datenbanken anzulegen, wenn die Daten bereits woanders vorliegen.

Ein einziges, verpflichtendes, offenes System für die Authentifikation, keine Insellösungen (von der Bank zum Fitnesscenter!).

Harte Strafen bei Datenschutzvergehen.

Totale Offenheit und damit Kontrolle über Datenzugriffe.

Investitionen in Breitbandausbau, allem voran im ländlichen Gebiet.

alpin

Im Echteinsatz?

Signatur Demo.

streamline your business

Remote signature – Vorteile

- Keine Hardware
- Keine Treiberinstallation
- Unkompliziert
- Mobile Nutzung und Nutzung im Browser
- Breite Anwendungsszenarien