Probably the best PKI in the world

PrimeKey At A Glance

- Solutions and Professional Services within Applied Cryptography with focus on PKI (what's PKI?)
- Main customers are Governments & Large Enterprises
- Headquarters in Stockholm, with offices in Sweden and Germany
- Developers and commercial force behind open source projects EJBCA.org and SignServer.org

PrimeKey Group

PrimeKey Solutions AB
Number of employees: 22
Date of incorporation: May 2002

PrimeKey Labs GmbH
Number of employees: 7
Date of incorporation: June 2012

100 years of PKI

- More than 100 years of collective experience in deploying real world, production, PKI systems.

- World-wide deployments. Europe, Asia, USA, Africa and Middle East.

- eID, ePassport, Government and Enterprise.

How We Started

- PKI is based on an ISO standard, X.509, complemented by multiple standards from IETF, Oasis, ETSI and other standardization organizations.
- Although there have been, and are some, patents around cryptography there are few barriers since the RSA patent expired in September 2000 (before this the US market was complicated).
- Many basic features of the standards were already available as open source software in 2001, when I started the EJBCA project.
    - The rest could be implemented and contributed back.

How We Started

- Implementing open standards in open source software, and contributing to other projects made it possible to implement the same functionality as expensive proprietary software as an open source project in 2001.
- In 2002 PrimeKey was started as a company to change the world of PKI.
- Today > 2000 downloads per month and thousands of deployments world-wide (one large partner made a survey claiming that 70% of governments operate EJBCA somewhere).
- EJBCA is now EJBCA Enterprise and EJBCA Community, trusted by governments and corporations for mission critical applications.

Who else?

- Security industry is largely dominated by large companies like RSA, Entrust-Datacard.
- In the PKI niche specifically there are several smaller companies in various countries in Europe (Sweden, Denmark, Germany, France, Spain, …)

This competition is possible with solutions based on open standards.

Implementing open standards

- Implementing open standards is low barrier.
  - Download standard documents.
  - Search for existing open source projects, with a suitable license.
  - Implement solution.
  - Interoperability test against open reference implementations.
- Short turn around
- Low cost
- Low barrier of entry

Implementing non-open standards

- Implementing non-open standards is high barrier.
  - If available, purchase standard document.
  - Implement from scratch.
  - Interoperability test against competitors or customers.
- Long turn around
- High cost
- High barrier of entry

Government customers ask us if we have nonopen standardization documents they can borrow, because the process is too heavy.

Result

- Governments and Enterprises have access to cost effective security solutions. PKI is nowadays underlying infrastructure of almost every secure communication technology.
  - Secure Web
  - VPN
  - Telco,mobile networks
  - eBanking
  - eInvoicing
  - IoT
  - …

No closed standards (except .doc) gets such ubiquitous presence.

What is EU doing good (1)?

- ETSI standards are open. Profiling PKI for use in EU with Trust Service Providers, eIDAS, etc.
- Allows competition between vendors in different countries.
- Possible to fulfill requirements based on ETSI standards across the world consistently.
  - Repetition lowers cost.

What is EU doing bad (1)?

- Enforcement takes a long time. Countries have been allowed to “add-on” national standards, making it very expensive to compete.
  - Allow(ed) local protection of markets.
- In our field the eIDAS regulation tries to relieve this, but it will take several years.
- ePassports...

ePassports

- In 2007 PrimeKey developed a second open source project, based on open standards, in order to deliver an ePassport solution to the Swedish Police.
- Implemented in record time, achieving an almost impossible time line where vendors of proprietary technology could not do it.

For ePassports there are two different standardization organizations, ICAO and EU, both unfortunately half-open/half-closed.
(does not fulfill requirements for an open standard according to the definition in EIF v1.0)

ePassports

- ICAO (works partly together with ISO).
  - Open standards documents.
  - Closed standardization process.
  - No/limited possibility for small companies to participate, except implementing the result.
- EU had a group called BIG, responsible for the first standard.
  - BIG group was terminated, BSI handles the standardization.
  - Open standards documents.
  - Close standardization process.
  - No/limited possibility for small companies to participate, except implementing the result.

ePassports

- BIG created a standard called SPOC.
  - No maintenance, still v1.0 although there are interoperability issues.
- EU requires member countries to implement the standard, threatening with fines.
  - But there is no maintenance of the standard. Implementation is very expensive and interoperability is very hard (the standard would benefit from a v2).
  - Leads to unnecessary high expenses for member countries, for little gain.
  - The standard is practically abandoned, but still enforced.

How could we do this?

- PrimKey is a supplier to the Swedish Police. As such we were close to the standardization, and could participate early on in the implementation.
  - Swedish police even contributed open source library implementing important parts of the semi-closed standard.
- Cert-cvc library, used in EJBCA, was born. Separate open source software, used by others across EU as well.

Basically, we were lucky.

Drawbacks

- Hard for independent vendors, without government connections to enter this market.
  - Suppliers in different countries with good connections had/have an advantage.
- Follow the biggest/most active country syndrome, hope they do the right thing for us as well?

Conclusions

- Open standards allow new disruptive companies to enter the market.
  - Improving technology
  - Lowering cost
  - Creating jobs
  - Does not threaten anything (except monopolies).
- EU can use the good standardization organs it has.
  - Don't let important projects bypass proper standardization.
  - Don't allow local additions for protecting local suppliers.
  - Require open standards for procurement.

Examples

- Contracting authorities in Sweden may require ICT standards as mandatory if these meet the requirement of the European Union’s Interoperability Framework (EIF v 1.0).

(https://joinup.ec.europa.eu/community/osor/news/sweden-refines-specifications-open-standards)

CSV (IETF), DNS (IETF), HTTP/S (IETF), IP (IETF), TCP (IETF), Date and time (ISO), PDF/A-1 (ISO), PNG (ISO), Genericode (Oasis), HTML (W3C), HTML5 (W3C), RDF (W3C), RDFa (W3C)

In our context...

- If procurement is performed requiring closed, or semi-closed, or regional, standards. Implementation will be costly and we will likely not be able to participate.
- If procurement is performed with open standards, we are likely to have implemented it already, and can deliver cost effective solutions.
  - In competition with other vendors EU-wide.
  - Extends to certifications required, not only technical standards.
- In our niche we are at least partly lucky, other areas may not be.

Requiring open standards (and avoiding region specific lock-in) in procurement can give large effects for SMEs.

PrimeKey & The ORIOS project

- important for **PrimeKey** to be at the **forefront of thinking** concerning development and use of open standards in software
- **partner** in a collaborative **research project** ORIOS (2012-2015)
- financially supported by the Knowledge Foundation

ORIOS: Overarching goal:

What are the necessary and desirable features of an Open Standard, and how can Open Standards and their implementations be utilised by small companies in different usage contexts?

UNIVERSITY
OF SKÖVDE

Knowledge Foundation

FINDWISE
SEARCH DRIVEN SOLUTIONS

PrimeKey

RedBridge