



AU2EU

Why we need privacy-preserving authentication in the FaceBook age

Dr Mike Johnstone, Edith Cowan University, AU



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no: 611659

Agenda



AU2EU

- **The problem**
- **Metadata kept by Facebook, Google etc.**
- **What is privacy-preserving authentication?**
- **A solution**
- **Video**

The Problem Space



- **Three themes**
- **Cyber crime**
- **The growth of the Internet**
- **The rise of individualism**

The Problem Space



- **The Internet of Things**
 - 28B devices by 2020 (helped along by IPv6)
 - Not just computers and phones
 - Home automation
 - Roadway sensors
 - Telemedicine
 - Cars
- **Cloud Computing**
 - Will hold 55% of all global data by 2017 (Cisco)
 - But where is it? (IP case study)

The Problem Space



- **Extent of cyber crime**
- **Cost of cyber crime**
- **Remedies**

Cyber Crime



- **Global cost of cyber crime \$119B in 2013**
- **Phishing scams**
- **Crypto-ransomware (targeted)**
- **Identity theft**



AU2EU

Sophisticated Phishing

Dear customer,

Your Apple ID was used to sign in to iCloud on an iPhone 6.

Time: November 06, 2015

Operating System: iOS 9.0.1

If you recently signed in to this device, you can disregard this email.

If you have not recently signed in to an iPhone with your Apple ID and believe someone may have accessed your account, please click here to confirm your details and change your password.

Apple Support

My Apple ID | Support | Privacy Policy

Copyright © 2015 iTunes S.à r.l. 31-33, rue Sainte Zithe, L-2763 Luxembourg. All rights reserved.

Cost of Cyber Crime

- **Direct**
 - Harvesting of credentials leads to financial loss
 - “I make \$600 dollars by working from home...”
 - But...banks are good at fraud detection
 - Poor passwords -> GPGPU Cube
- **Indirect**
 - Cost to recover from loss of information
 - Loss of competitive advantage
 - Goodwill
 - Stock price
 - ...

Cost of Cyber Crime



- **Reported incidents growing**
- **Unsurprisingly, spending growing as well**
- **The cyber security industry is growing at a rapid rate with worldwide spending expected to reach US\$86 billion by 2016**

User behaviour

(Symantec, 2015)



- **An alarming percentage of apps collect and send personally identifiable information to app developers**
- **Many consumers are willing to allow apps access to their personal information**
 - **68% of people will willingly trade their privacy for a free app**
- **App users think they understand what they are agreeing to when downloading apps**
 - **In reality, they have little understanding of common app permission practices and behaviours**
 - **Over half of survey respondents were unaware that apps could track their physical location**
 - **22% of apps scanned by Norton Mobile Insight track location**



Rise of individualism

- **Oration vs. Reason**
- **Anti-Intellectualism in American Life (Hofstadter, 1963)**
- **Evangelism vs. Intellectualism**
- **The Scopes trial (USA, 1920s)**
 - **Few Tennesseans believed in evolution**
 - **Undemocratic for a few rationalists to push their views onto the masses**
- **Most people are happy to say “<insert my country here> is the most anti-intellectual in the world”**
- **This is not a new phenomenon**

Leading to Denialism



- **Climate change**
- **Vaccination (the anti-vaxer movement)**

- **The resilience and permanence of the Internet does not help here**



Authentic Anecdotes

- Facebook
- Twitter
- Bloggers
- Talk shows
- Media campaigns
- The triumph of the personal anecdote over reason and science
- “Don’t let actual data get in the way of a good story”

Views on Privacy



- **Privacy is not a new idea (unlike the concept of the individual)**
 - Privacy is at least 30 000 years old (which culture is that)?
- **“Privacy is Theft” (The Circle by Dave Eggers)**
- **Sometimes it might be good to know someone’s location (Captial case)**
- **Loyalty cards and mass customisation (Profiling case)**
- **The gathering of large amounts of data leads to unforeseeable uses of said data**
- **Recent changes to metadata laws in Australia**
- **Australian Law Reform Commission report on Privacy (2008) runs to 2700 pages with 295 recommendations for change**



AU2EU



SOCIAL MEDIA
In Business



Popular Social Networking Sites

(www.statisticbrain.com, 2015)

- Facebook 1,440,000,000
- Google+ 347,000,000
- LinkedIn 336,000,000
- Instagram 302,000,000
- Twitter 289,000,000
- Tumblr 237,000,000
- Snapchat 113,000,000
- Pinterest 73,500,000

Facebook

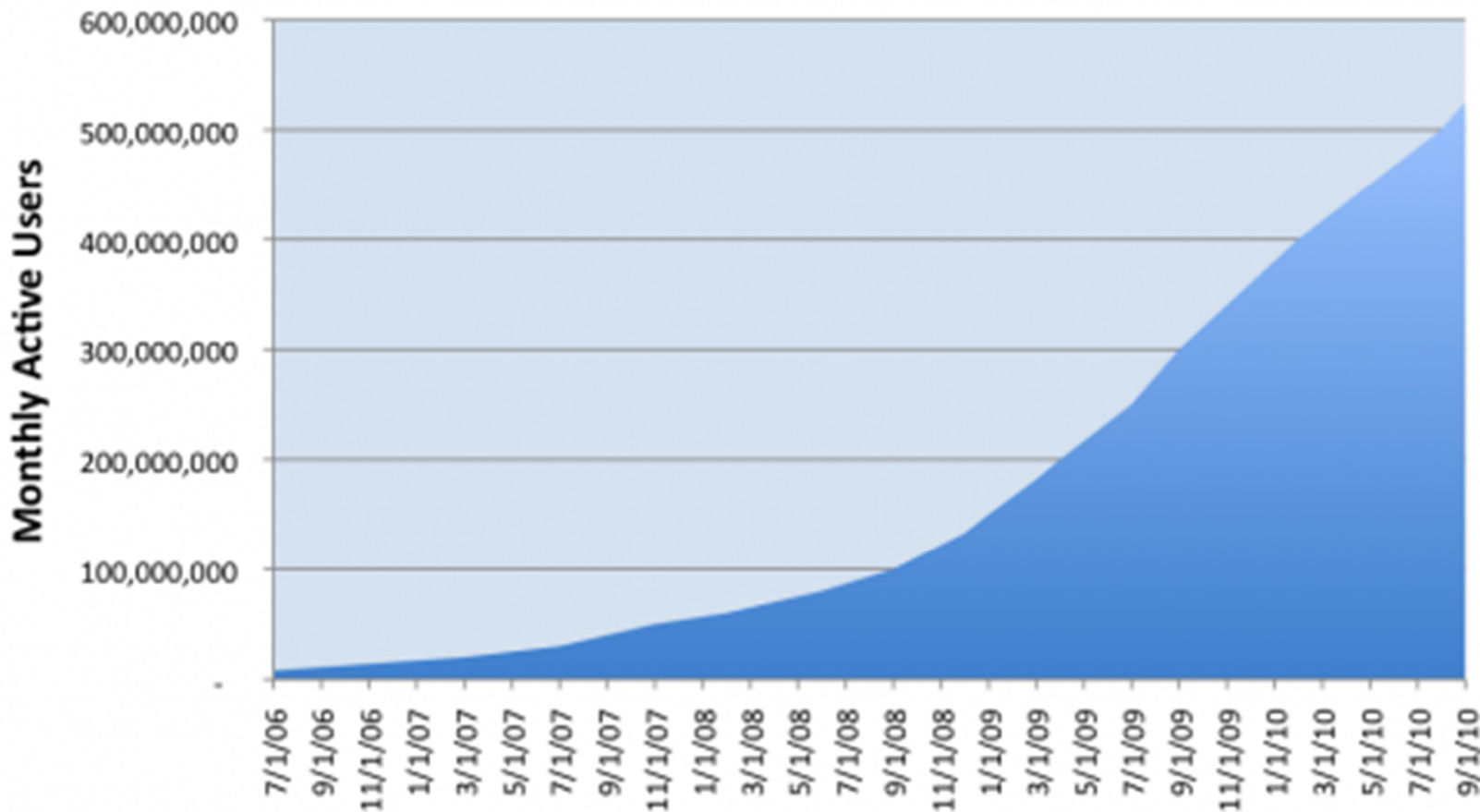


- **Worldwide, there are over 1.44 billion Facebook users**
- **In Europe, over 307 million people are on Facebook**
- **Every 60 seconds on Facebook:**
 - **510 comments are posted**
 - **293,000 statuses are updated**
 - **136,000 photos are uploaded**
- **There are 83 million fake profiles**

Rate of Growth of Facebook

Facebook Worldwide User Growth, 2006-2010

InsideFacebook.com



Source: Facebook announcements



AU2EU



Web connections



- **When a browser issues an HTTP GET request, there will be a log entry in the destination web server**
- **If the page contains multiple content items from different sites, there will be a log entry on every server that sends back an HTTP Response**
- **What might be in a log entry?**
 - **Your IP address**
 - **Timestamp**
 - **The GET Request**
 - **Web browser type/version**
 - **OS version**

Browser disclosure

- **Cookies**
 - Great for a seamless browsing experience
 - Can only be sent to the issuing domain
 - But...uniquely identify a user
- **HTTP Referer (not referrer) data**
 - Click on a link and the destination knows where you are coming from
 - If you are using Google, the search terms are disclosed twice (once to Google and once to the destination)

Facebook and Privacy



- **Facebook privacy policy likely to be counter to EU law**
- **Data scraping via public APIs a problem**
- **Facebook's ability to track users' activity outside Facebook has increased over time**
 - **Via the spread of "Like" buttons and through new forms of mobile tracking (see below)**
- **Facebook now gathers information through these plugins regardless of whether the buttons are used.**
- **Instagram and WhatsApp now owned by Facebook**
 - **Can now collect more user data, which enables more detailed profiling**

Facebook, image sharing and location



- **Direct upload**
 - No metadata stored, but metadata is recorded prior to being stripped from an image and made available via the account data file
- **Cross-post from 500px, Flickr, Pinterest**
 - Revealed full Exif metadata
 - GPS coordinates retrievable

While we are here: Google



- **Gmail**
- **AdSense**
- **AdWords**
- **DoubleClick**

Anyone else? Viber

- Popular phone/messaging app
- 664M users (www.statista.com, 2015)
- Sends/stores data in unencrypted form (since claimed to be fixed)
- Potential privacy issues:
 - Read SMS, that's any message (even non-Viber messages, from your SIM card)
 - Read phone log data – potentially personal or private information
 - Read your contacts and move them to their server
 - Read your location
 - Record audio, take pictures and videos
 - Automatically start when your phone is switched on

Effect of the Internet on Privacy

- In 1993, there were 130 websites, now there are over 954 million (<http://www.internetlivestats.com/total-number-of-websites/>)
- Smart phone cameras
- Public surveillance cameras
- Drones (with cameras, of course)
- What do younger generations think about this?
 - The ALRC was not sure
 - Folly of youth
 - Loosening of attitudes toward privacy
- Stigma reversal
 - Certainly an effect in Australia

Legal remedies



- **Logical to assume data ownership sits within national boundaries**
- **The Microsoft vs. US Govt. case said otherwise**

History refresher

- **Cardinal Richelieu (1585-1642)**
- **Dominated France from about 1624 as the Chief Minister for Louis XIII. He was considered one of the great French politicians**
- **Adhered to the maxim**

‘The ends justifies the means’

which has relevance to the American Government’s use of warrants as illustrated in the Microsoft Email Case



History refresher



- **Cardinal Richelieu also said**

“...If you give me six lines written by the most honest man, I will find something in them to hang him...”

- **Microsoft E-Mail Case...a new way to get information in secret – (Richelieu's six lines) – what could be misinterpreted from your email contents?**



Moving on to a bit of Law

- **Jurisdiction**
- **Mutual Legal Assistance Treaties (MLAT).**
- **Warrants – search...subpoenas...warrant issued under the Electronic Communications Privacy Act**
- **Interaction between legal process and law (the Microsoft warrant – a process - is also jointly covered by various American laws including section 108 of the Patriot Act, Stored Communications Privacy Act...**
- **In particular, emphasis was placed on the meaning of the words “where the property is located” being the location of the ISP, not the location of any server**

Implications



- **‘where the property is located’**
- **Office in America but content in Ireland.**
- **Raises a conflict for Microsoft – comply with American law and probably breach EU/Irish law...steps around MLAT**

Privacy-Preserving Authentication



- **We want to connect to many disparate systems seamlessly**
- **...but we don't want to give away our whole life story**
- **PPA allows us to verify claims without needing details**

Secure Privacy-Preserving Authentication



- Privacy:
 - Unlinkable transactions
 - Minimal information disclosure
 - Offline issuer
- Security
 - Impersonation impossible
 - Accountability
- Efficient and mature solutions for Privacy-ABCs **exist** and **are freely available**
 - IBM's Identity Mixer
 - Microsoft's Uprove



Anonymous credentials



- A user doesn't transmit the credential but proves that s/he poses it (verifier cannot reuse the credentials)
- The user can reveal the selected set of attributes
- The user can prove that some complex predicate over the attribute holds (e.g. older than 18 years)
- Zero-footprint deployment regarding users
- Excellent compromise between user control, privacy, and ease of deployment

Authentication and Authorisation for Entrusted Unions

Project Acronym: AU2EU

Grant agreement no: 611659

Funded under: FP7 (Seventh Framework Programme)

Call (part) Identifier: FP7-ICT-2013-10

Total Budget: 8,696,539 (€)

Start Date: 2013-12-01

Duration in months: 24















AU2EU



**SEVENTH FRAMEWORK
PROGRAMME**

Consortium Members

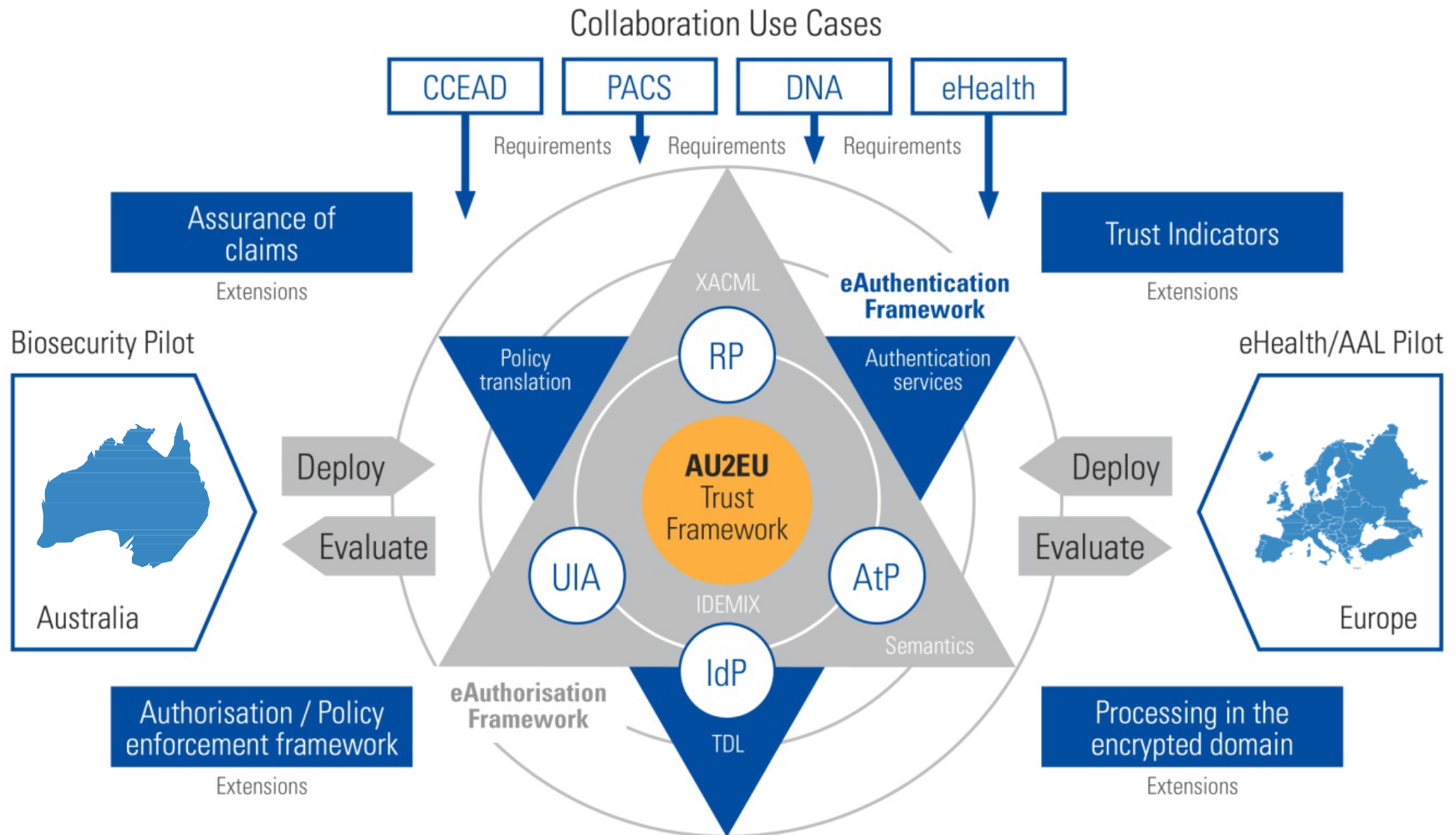
<p>Eindhoven University of Technology</p> 	<p>Philips Electronics Nederland B.V.</p> 	<p>Bicore Services B.V.</p> 
<p>NEC Europe LTD</p> 	<p>IBM Research GMBH</p> 	<p>German Red Cross E.V.</p> 
<p>Thales Communications & Security SAS</p> 	<p>Commonwealth Scientific and Industrial Research Organisation</p> 	<p>Edith Cowan University</p> 
<p>Royal Melbourne Institute of Technology</p> 	<p>University of New South Wales</p> 	<p>Macquarie University</p> 

Project Aims



- **Integrated eAuthentication and eAuthorisation framework**
 - Privacy-preserving
 - Cross-domain
- **A user can choose to reveal a selected set of attributes**
- **Platform development and deployment in two pilots**
- **Advancing the state-of-the-art in:**
 - assurance of claims
 - policy enforcement
 - trust indicators
 - operations in an encrypted domain

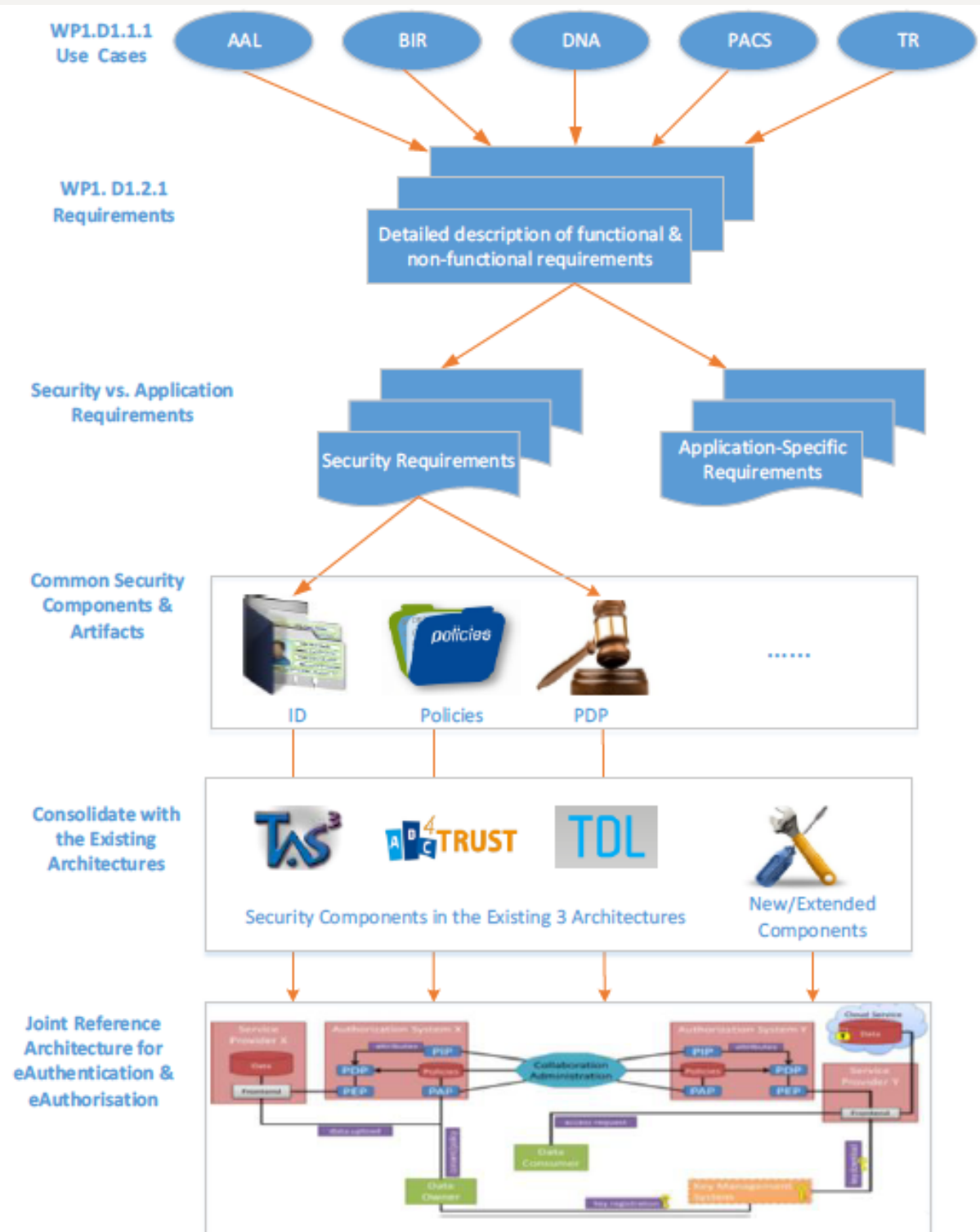
Project Structure



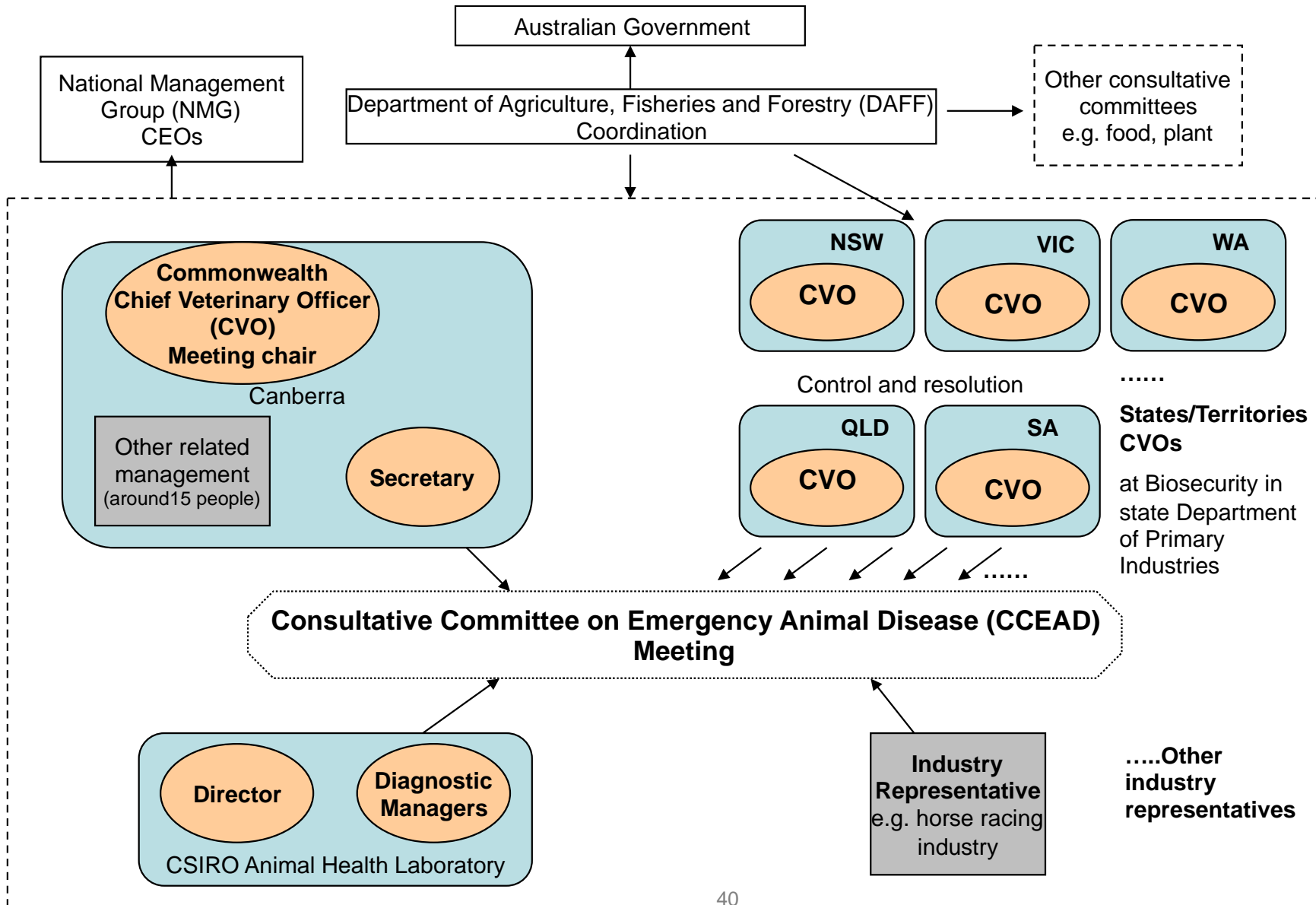
Reference architecture

Fundamental concepts:

- Composable architecture
- Open to technology and standards evolution
- Attributes remain with the source of the data
- User consent/privacy preferences
- Privacy
- Correctness and accountability

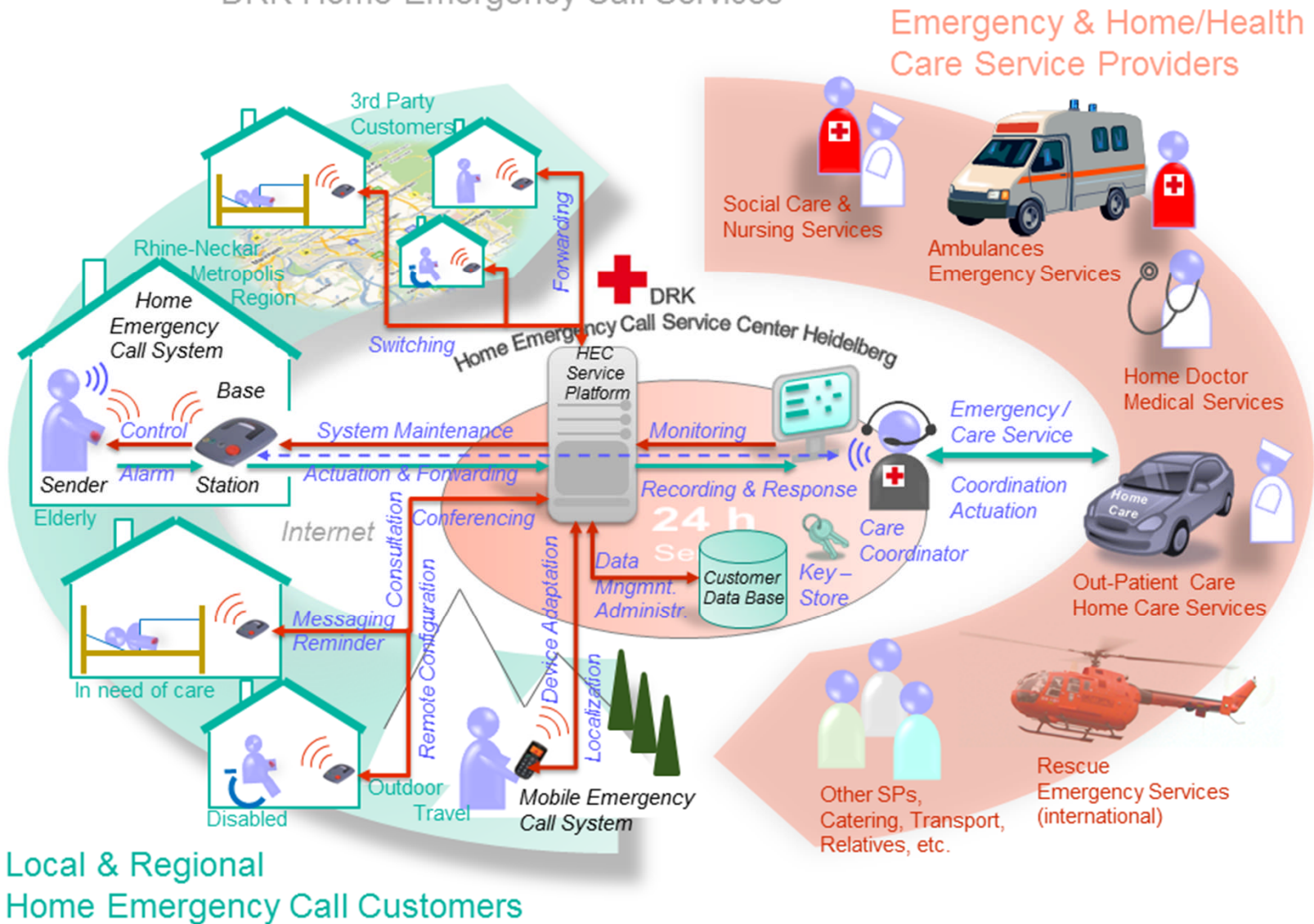


Biosecurity Pilot



eHealth Pilot

DRK Home Emergency Call Services





Some final words

- **“I am a human being, and all things which concern human beings concern me”**

Publius Terentius Afer (Terence) 195/185-159 BCE

- **Who, then, owns the record of my life, or yours?**