

Intuitive and Sensible Access Control Policies

NOKIA

N. Asokan

Early days of automobile safety



Courtesy:

<http://www.scienceandsociety.co.uk/results.asp?image=10326966&wwwflag=2&imagepos=4>

http://en.wikipedia.org/wiki/Locomotives_and_Highways_Act

- **UK Locomotives and Highways Act (1856) to assure safe driving**
 - **Man with a red flag or lantern 55 m in front of the car to warn**
 - **Max. speed in towns: 3.2 km/h**
- **Revised in 1878**
 - **Red flag man only 18 m in front**
 - **Widely ignored**
- **Repealed in 1896**

Automobile safety today



- The human is still in control
- Not just better “user interaction”
- But several underlying new technologies are in use
 - Traffic lights
 - Air bags
 - Anti-lock breaks

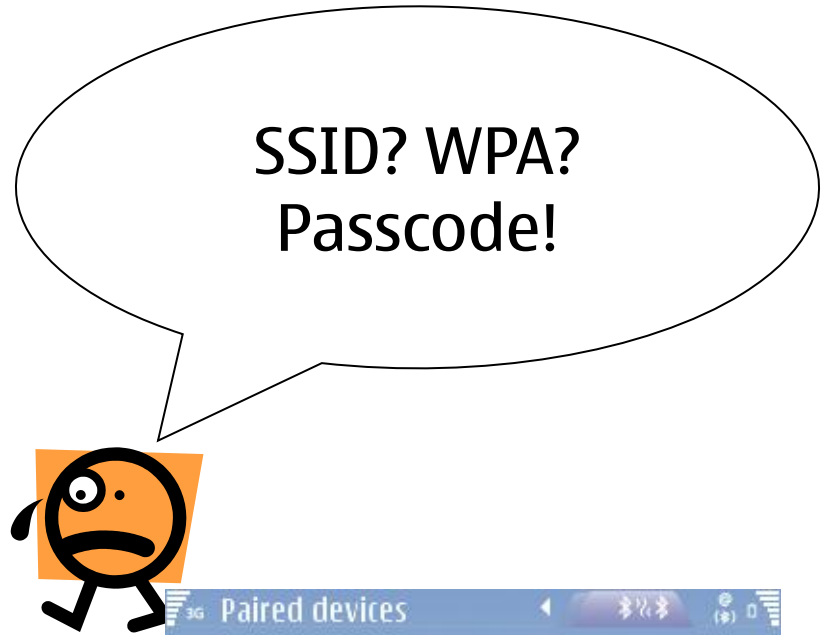
"People are still doing dumb things. But the fact is, the cars are now much safer and are more likely to save them. A crash that might have killed you 20 years ago is probably very survivable now."

Courtesy:

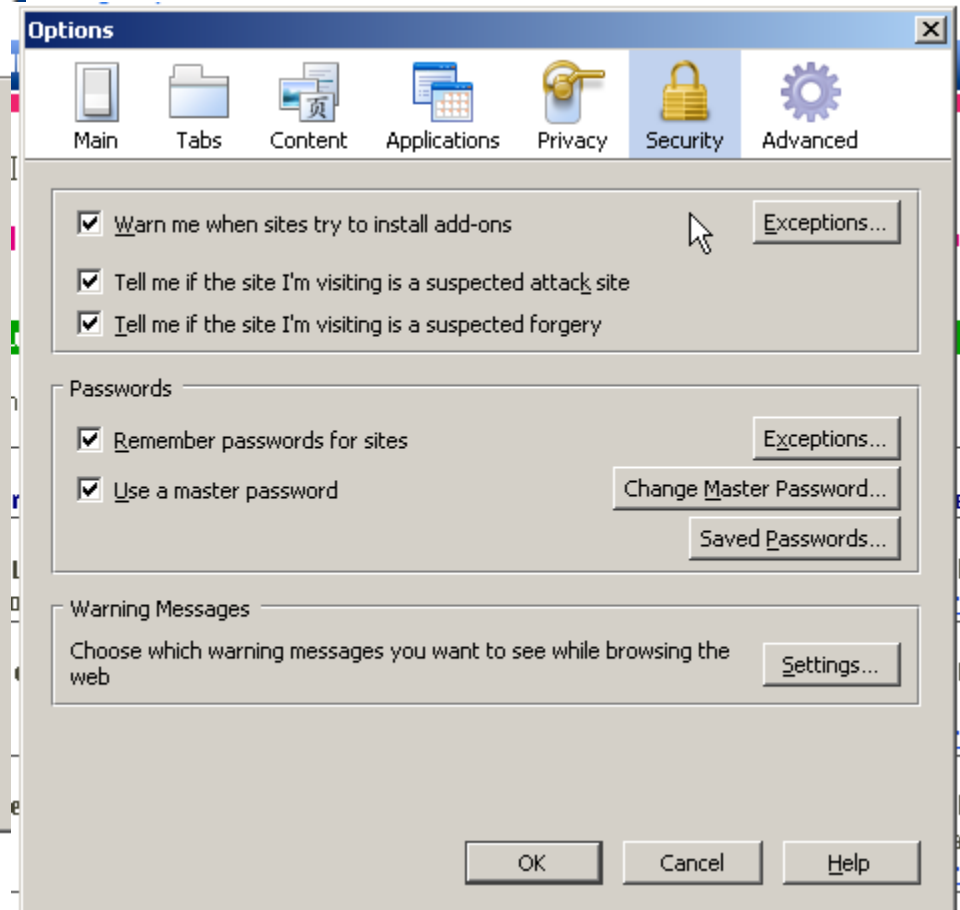
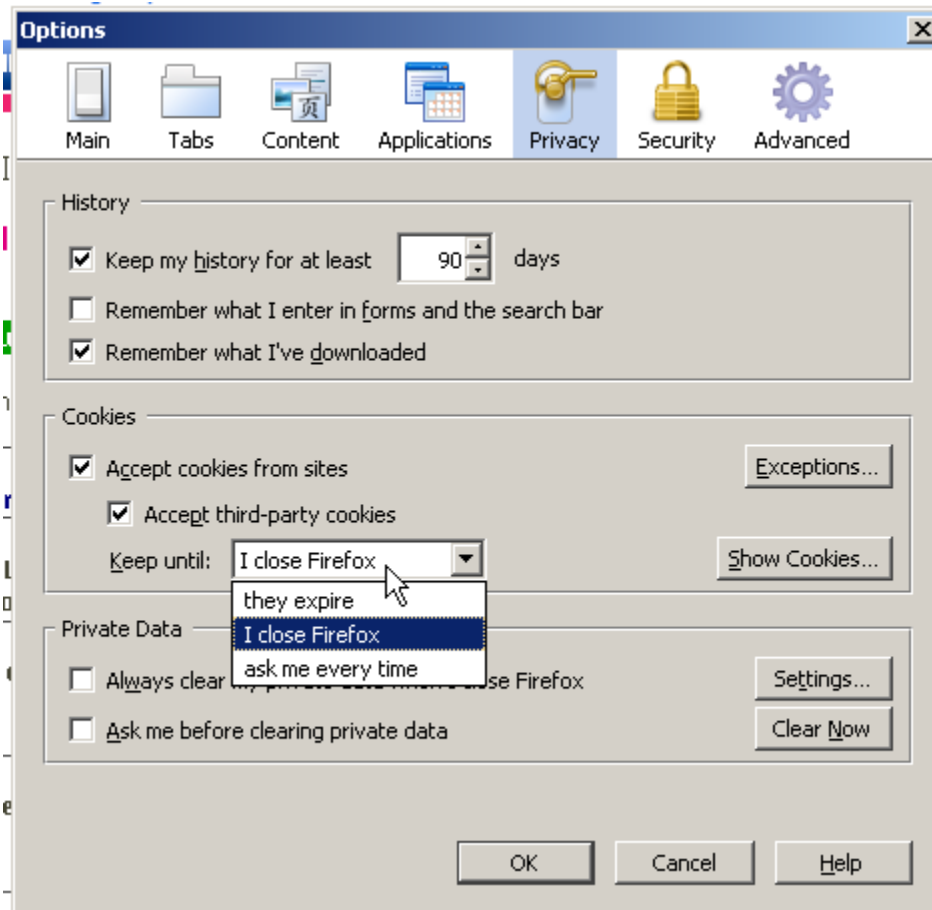
http://research.cars.com/go/advice/Story.jsp?section=safe&subject=safe_tech&story=techIntro

http://research.cars.com/go/advice/Story.jsp?section=safe&subject=safe_tech&story=techOther&referer=advice&aff=national

Early days of secure communication (today!) ~~today!~~



Early days security policies for the masses (today!)



Policy-by-drudgery: set precise and detailed policies manually

[Privacy](#) ▸ Applications

Overview

Settings

What Other Users Can See via the Facebook Platform

When a friend of yours allows an application to access their information, that application may also access any information about you that your friend can already see. [Learn more](#).

You can use the controls on this page to limit what types of information your friends can see about you through applications. Please note that this is only for applications you do not use yourself:

Share my name, networks, and list of friends, as well as the following information:

- | | |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Profile picture | <input checked="" type="checkbox"/> Events I'm invited to |
| <input checked="" type="checkbox"/> Basic info What's this? | <input checked="" type="checkbox"/> Photos taken by me |
| <input checked="" type="checkbox"/> Personal info (activities, interests, etc.) | <input checked="" type="checkbox"/> Photos taken of me |
| <input checked="" type="checkbox"/> Current location (what city I'm in) | <input checked="" type="checkbox"/> Relationship status |
| <input checked="" type="checkbox"/> Education history | <input checked="" type="checkbox"/> Online presence |
| <input checked="" type="checkbox"/> Work history | <input type="checkbox"/> What type of relationship I'm looking for |
| <input checked="" type="checkbox"/> Profile status | <input type="checkbox"/> What sex I'm interested in |
| <input checked="" type="checkbox"/> Wall | <input type="checkbox"/> Who I'm in a relationship with |
| <input checked="" type="checkbox"/> Notes | <input type="checkbox"/> Religious views |
| <input checked="" type="checkbox"/> Groups I belong to | |

Do not share any information about me through the Facebook API

Applications Authorized to Access Your Information

When you authorize an application, it can access any information associated with your account that it requires to work. Contact Information is never shared through Platform. You can view a full list of applications you have authorized on the [Applications](#) page.

Facebook Connect Applications

**Information about Recent Activity**[close](#)

Whether we display a story on your profile is now controlled by the privacy of the content itself, rather than an additional setting. For example, only people who can see both your Wall, and the Wall to which you posted would be able to see a story about you writing on a friend's Wall. You cannot completely turn off recent activity stories anymore. However, if you want to remove a particular story that currently shows up, simply click the "Remove" button that appears to the right of the story after you move your mouse over it. [Learn more about privacy here.](#)

Privacy Settings ▶ Profile Information[← Back to Privacy](#)[Preview My Profile...](#)**About me**

About Me refers to the About Me description in your profile

Everyone

Personal Info

Interests, Activities, Favorites

Only Friends

Birthday

Birth date and Year

Family, close-relatives, clo...

Religious and Political Views

Only Me

Family and Relationship

Family Members, Relationship Status, Interested In, and Looking For

Family, close-relatives

Education and Work

Schools, Colleges and Workplaces

Only Friends

Photos and Videos of Me

Photos and Videos you've been tagged in

Only Friends

Photo Albums[Edit Settings](#)**Posts by Me**

Default setting for Status Updates, Links, Notes, Photos, and Videos you post

Family, close-relatives, clo...

Allow friends to post on my Wall Friends can post on my Wall**Posts by Friends**

Control who can see posts by your friends on your profile

Family, close-relatives, clo...

Comments on Posts

Control who can comment on posts you create

close-relatives, family, clo...



Policy-by-fiat: No choice - defaults specified by developer/administrator

Current state of access control policies

Today the choice for ordinary users is *between* “sensible” and “intuitive”

Problem:

How can ordinary users set
and manage access control policies?

Objective:

Intuitive means to set/manage
sensible access control policies

How do users set access control policies?

Eventually...

Policy-by-inference: trusted assistant

Tomorrow

Policy-by-imitation: “do what he/she does”

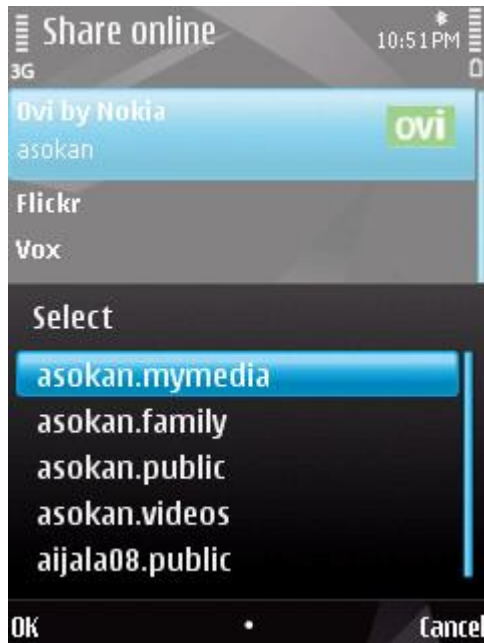
(Andreas Heiner; also see [“Privacy Suites” by Bonneau et al](#), SOUPS 2009)

Today

Policy-by-fiat: developer/administrator-set defaults

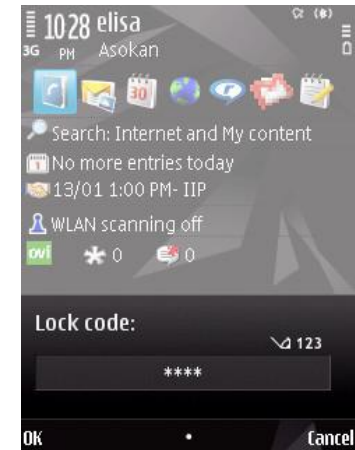
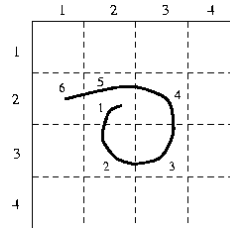
Policy-by-drudgery: user suffers through fine-grained policies

Example 1: privacy settings for photo channels

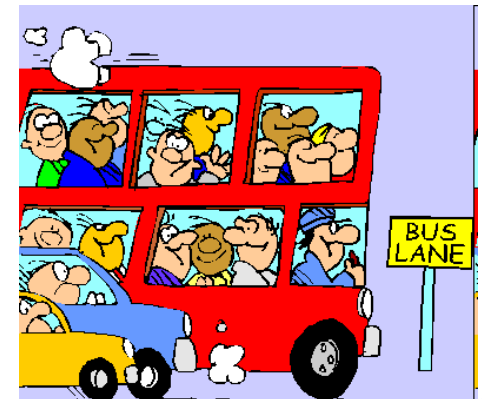


Can we select a sensible default channel based on the data and metadata to be uploaded?

Example 2: authentication for screensaver unlocking



What local authentication method to use when?



Questions

- What applications and what kinds of access control policies?
 - Device lock policy, application privileges
 - Privacy policies for sharing data with others
 - ...?
- How do we set initial policy?
 - User-chosen cluster, Segmentation-by-querying-user, Policy-by-imitation, ...
 - Clustering users based on initial user behaviour and other context information?
- How do we evolve policies?
 - Clustering objects (data), user feedback (e.g., using non-modal dialogs – “OmbudsKey”)
- How to get the data for clustering?
 - Clustering for policy initialization requires access to other people’s policies
 - Access control policy not as sensitive as personal data: users more willing to share them?
- What is so special about security/privacy policies?
 - Cost of incorrect inferences
 - ...?

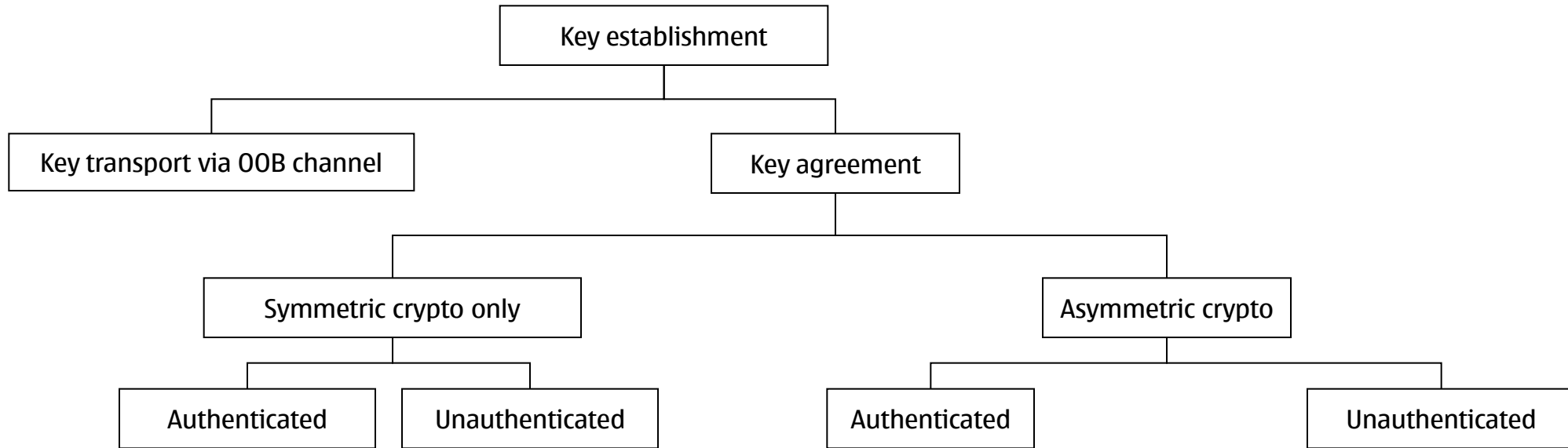
What happened to the first problem?

- Several research papers by various researchers
- Several new standards specifications (2005-2007)
- Deployment in progress: products hitting the market now

Wanted: Secure, intuitive, inexpensive first connect

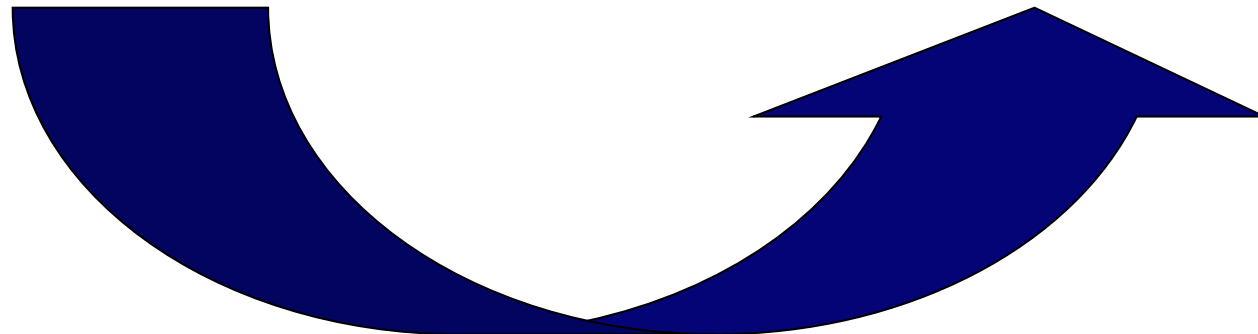
- Two (initial) problems to solve
 - Peer discovery: finding the other device
 - **Authenticated key establishment:** setting up a security association
- Assumption: Peer devices are physically identifiable

Key establishment protocols for first connect (1)



Short keys vulnerable to passive attackers

Secure against passive attackers



Authentication by comparing short strings

Choose long random R_A

Calculate commitment

$$h_A \leftarrow h(A, R_A)$$



key agreement: exchange PK_A, PK_B



Choose long random R_B

Verify commitment

$$h'_A \stackrel{?}{=} h(A, R'_A)$$

Abort on mismatch

$$v_B \leftarrow H(A, B, PK'_A | PK_B, R'_A, R_B)$$



$$v_A \leftarrow H(A, B, PK_A | PK'_B, R_A, R'_B)$$



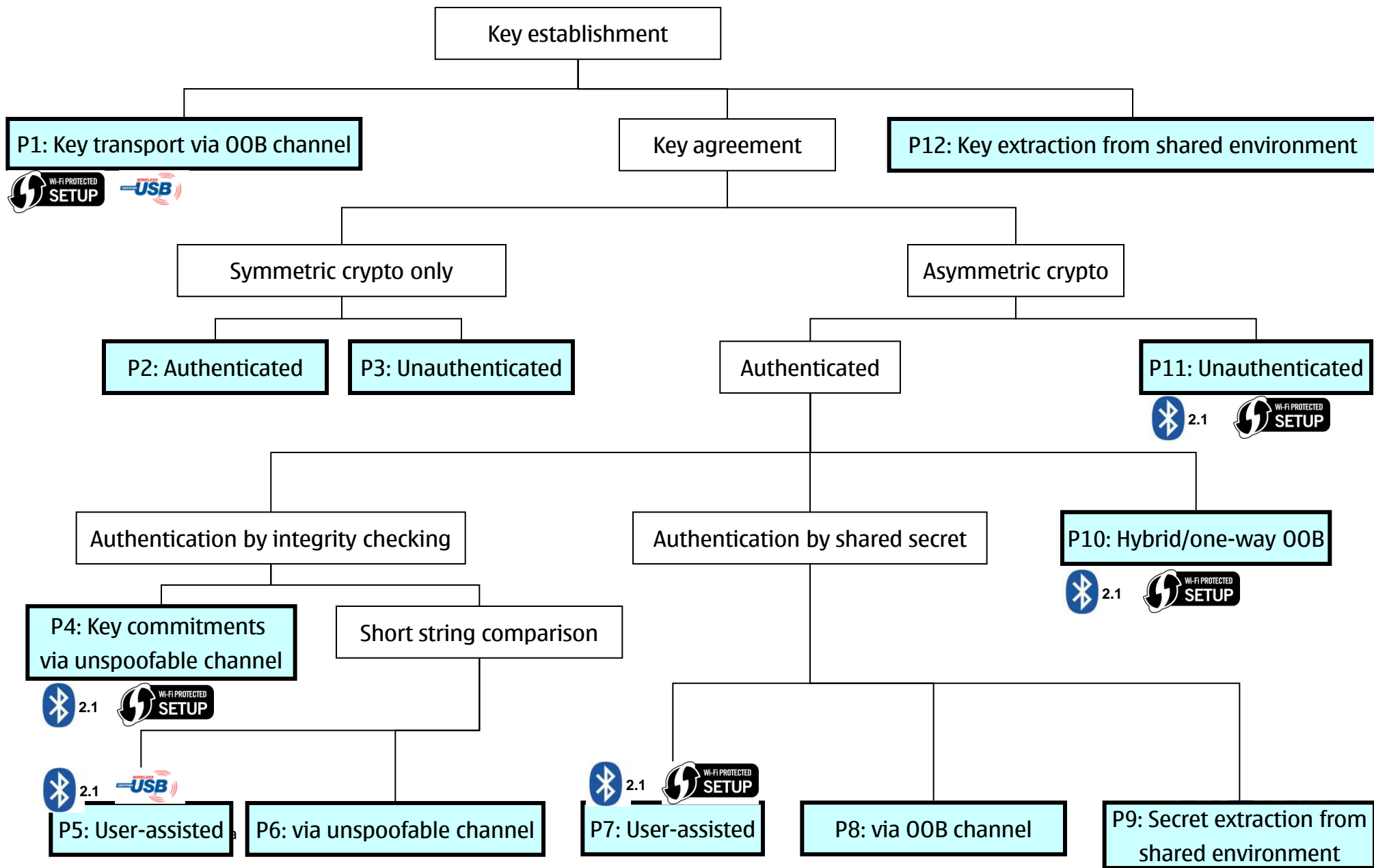
User approves acceptance if v_A and v_B match

2^{-l} (“unconditional”) security against man-in-the-middle (l is the length of v_A and v_B)

$h()$ is a hiding commitment; in practice SHA-256

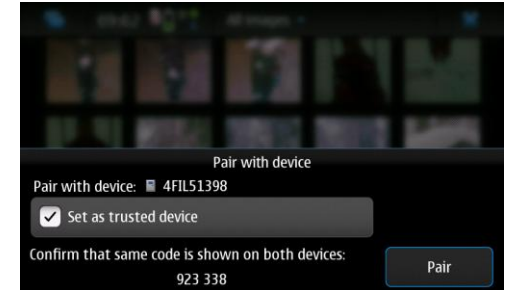
MANA IV by Laur, Asokan, Nyberg [\[IACR report\]](#) Laur, Nyberg [\[CANS 2006\]](#)

New Standards for first connect

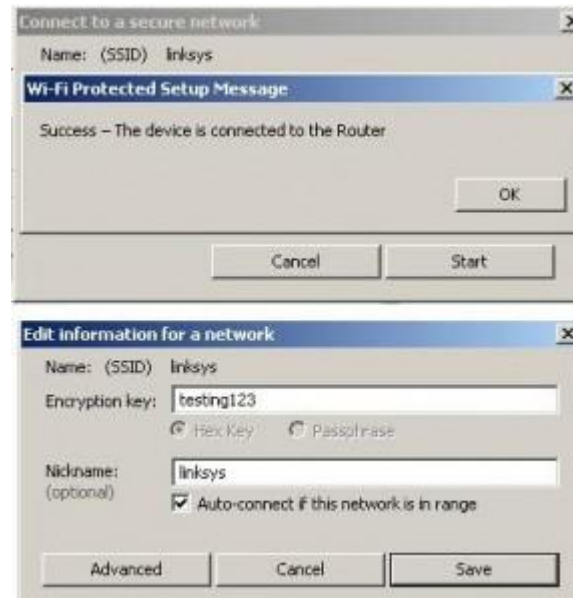


Deployment in progress

- Secure Simple Pairing  2.1



- WiFi Protected Setup 



NOKIA

Outlook for the future

- Need to revisit Secure First Connect?
 - Unauthenticated key agreement may be the winner: cost and usability
 - But some scenarios would require authentication: input devices, medical devices?
 - “Wanted: inexpensive, intuitive, secure techniques for first connect”?

- Extending First Connect
 - Beyond security associations
 - How can users easily specify access control policies?
 - Group first connect