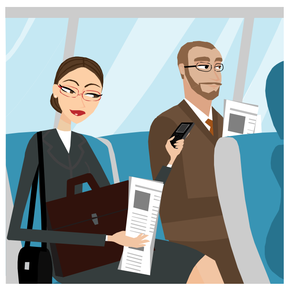
Marcin Nagy[1], N. Asokan[2,3], Jörg Ott[1]
[1]Department of Communication and Networking, Aalto University, Finland
[2]Department of Computer Science, University of Helsinki, Finland
[3]Department of Computer Science and Engineering, Aalto University, Finland

Proximity social interactions

WHY?

Often we want to know answers to these questions:

Can I share my ride with him?



Who will let me tether through their phone?

Do I know anyone here?

WHAT?

Solving this challenges requires:

SECURITY AND PRIVACY

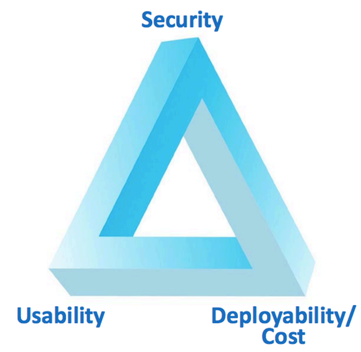
- **Authenticity:** no false claims possible
- **Secrecy:** secure information data are transfer
- **Privacy:** only common features revealed

PERFORMANCE AND USABILITY

- Time and energy-efficient operations
- Applicable in mobile scenarios

DEPLOYABILITY

- Easy integration with existing social networks



HOW?

BOOTSTRAPING FROM SOCIAL NETWORKS

Take advantage of existing online social networks:

- Single Sign-On and OAuth
- Access policies using social relationships
- Social graph to learn about other users

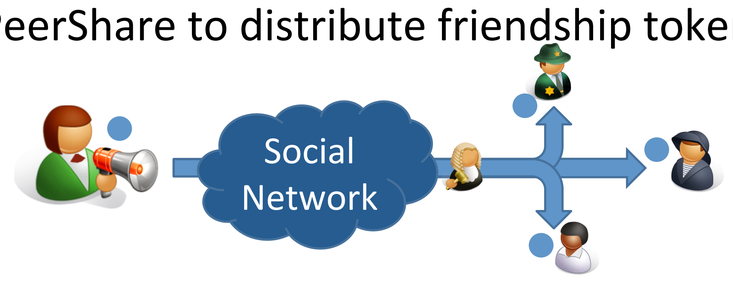
PEERSHARE

Distribution of sensitive data among social contacts:

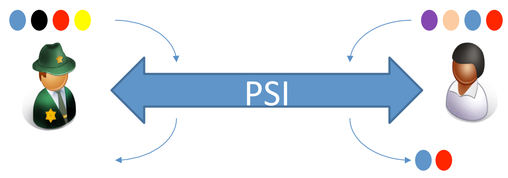
- User can specify authorized recipients intuitively
- Different types of protection supported
- User and application access control enforced
- **Android** implementation with simple to use API*

FINDING COMMON FRIENDS

1. Use PeerShare to distribute friendship token:



2. Use Private Set Intersection (PSI) on token sets to find common friends:



- Bloom Filter based PSI improves efficiency
- Applicable also for mobile scenarios
- Quick completion time
- Low energy consumption
- **Common Friends Framework** abstracting away crypto complexity from app developers*

REFERENCES

1. *PeerShare: A System Secure Distribution of Sensitive Data Among Social Contacts*, NordSec 2013
2. *Do I Know You? – Efficient and Privacy-Preserving Common Friend-Finder Protocols and Applications*, ACSAC 2013

*code available on request