



Future Cryptographic Requirements from Mobile Applications

Chris Mitchell, Kenny Paterson
and Vaia Sdralia
Information Security Group,
Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, UK.



Some Trends in Mobile Telecoms



- > Advent of 3G networks
- > Legacy of GSM networks
- > Ad hoc wireless networking
 - > 802.11 and Bluetooth today
 - > moving to truly *ad hoc* and heterogeneous networks in the future
- > Continued miniaturisation leading eventually to sensor technologies and Body Area Networks (BANs)

27/11/2002

STORK presentation



Some Challenges

Constraints:

- > Limited chip areas
- > Low power consumption, processing power, and code size

And yet:

- > High bandwidth applications (data not voice)
- > *Ad hoc* authentication and network access control
- > Mobile services: payment, DRM, location-based,...
- > Privacy issues associated with context aware services

27/11/2002

STORK presentation



Implications for Cryptography

Q: So what does this mean for cryptography?

A: A need for research in:

- > Lightweight encryption techniques
- > Lightweight public-key techniques
- > Privacy control management
- > Delegation and distribution protocols
- > Multicast key management

27/11/2002

STORK presentation



Lightweight Encryption

- > Link-level confidentiality:
 - > A5 stream ciphers in GSM (mid 80's)
 - > Block cipher Kasumi mode of operation in 3G systems (mid-late 90's)
- > Future 'ultra-portable' systems may need to revert to lightweight stream ciphers
- > Few public proposals with well understood **and** acceptable security level
- > NESSIE has begun the process of identifying candidates

27/11/2002

STORK presentation



Lightweight Public-Key Techniques

- > 3G standards do not make use of public-key cryptography
- > Systems beyond 3G will use PKC:
 - > payment, digital rights management, mobile code management,...
- > Need for continued research in lightweight PK algorithms and protocols
- > Need for PKI suited to mobile environment, implemented on SIM/USIM
- > Alternatives to X.509-based PKIs: ID-PKC, SPKI, empowerment model

27/11/2002

STORK presentation



Privacy Control Management

- > Context aware services can be based on:
 - calendar data, user location data, social context, personal preferences, type and status of network infrastructure,...
- > Apparent conflict with users' privacy rights and expectations...
- > ... in conflict with law enforcement requirements
- > There are some pointers in the research literature:
 - > Escrow techniques
 - > Brands' limited show certificates
 - > Blind signatures, deniable signatures
 - > Anonymous e-cash
- > Again, **lightweight** should be the watchword

27/11/2002

STORK presentation



Delegation/Distribution Protocols

- > Low power device may need to delegate complex cryptographic processing, eg digital signature computation
- > From SIM/security token to local mobile device, or to another device on same PAN/BAN
- > Delegatee may be untrusted, so delegation must proceed without revealing secret
- > Possibly in distributed fashion: spread task over multiple devices
- > Large existing literature on server-aided RSA computation needs re-examination

27/11/2002

STORK presentation



Multicast Key Management

- > Trend towards integrating broadcast/multicast and mobile wireless technologies
- > Proprietary content, so content and context needs authentication, encryption and integrity protection
- > Group/broadcast key management problems – need for efficient distribution, group enrollment and disenrollment protocols.

27/11/2002

STORK presentation

