# Demo Overview: Fully Decentralised Authentication Scheme for ICN in Disaster Scenarios (Demonstration on Mobile Terminals)

Jan Seedorf, Bilal Gill, and Dirk Kutscher
NEC Laboratories Europe
Heidelberg, Germany
jan.seedorf@neclab.eu,
bilal.gill@neclab.eu,
dirk.kutscher@neclab.eu

Benjamin Schiller and Dirk Kohlweyer
Technical University of Darmstadt
Darmstadt, Germany
schiller@cs.tu-darmstadt.de,
dirk@kohlweyer.net

## ABSTRACT

Self-certifying names provide the property that any entity in a distributed system can verify the binding between a corresponding public key and the self-certifying name without relying on a trusted third party. However, self-certifying names lack a binding with a corresponding real-world identity. In this demonstration, we present the implementation of a concrete mechanism for using a Web-of-Trust in conjunction with self-certifying names to provide this missing binding. Our prototype runs on Android devices and demonstrates a decentralised message authentication scheme for any kind of content-oriented architecture. In the demonstration, we show how our proposed scheme performs—in terms of time needed to assess the trustworthiness of information retrieved—in a fully decentralised scenario: fragmented (mobile) networks. In such a scenario, connectivity to centralized authentication entities and Web-of-Trust key-servers is not available. Our scheme is hence executed solely on end-user terminals itself (which have limited processing capabilities).

## 1. INTRODUCTION

*Self-certifying names* provide the useful property that any entity in a distributed system can verify the binding between a corresponding public key and the self-certifying name without relying on a trusted third party [3]. This is normally achieved by basing the self-certifing name (in some way) on the pre-image resistant hash of the corresponding public key. Self-certifying names are very useful for addressing the security requirements in *Information Centric Networking (ICN)* architectures: Any source can append a public key and a digital signature (computed with the corersponding private key) to a data item which belongs to a self-certifying name, and any intermediate entity (e.g. an ICN-router/Cache) or any receiving entity (i.e. the issuer of an interest for the self-certifying name) can verify the signature with the received public key. The binding between public key and self-certifying name can be verified by anybody, without relying on a trusted third party or a *Public Key Infrastructure (PKI)*. There is thus no need to authenticate the identity of the host that caches an object; the approach does not follow today's *host-centric* security but is inline with ICN's propagated *data-centric* security paradigm. Self-certifying names thus provide a decentralized form of data origin authentication and are very useful in ICN architectures. However, self-certifying names lack a binding with a so-called *Real-World Identity (RWI)* [4]: While the concept enables to verify that whoever signed some data was in possession of the private key associated with the self-certifying name, it does not provide any means to verify what real-world identity corresponds to the public/private key pair, i.e. who actually signed the data [4].

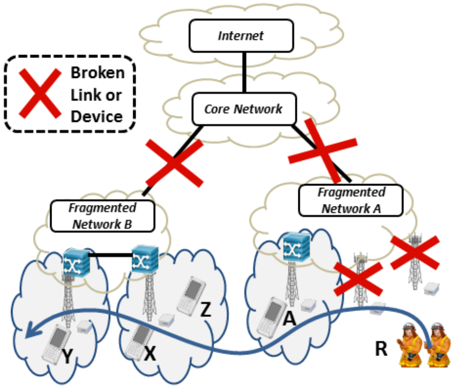

**Figure 1: Mobile Network after Disaster with Fragmented Networks [5]**

In this demonstration, we present our prototype implementation of a concrete mechanism we have proposed previously [5] for using a Web-of-Trust (WoT) in conjunction with self-certifying names to provide precisely this RWI-binding. We consider a decentralised scenario: fragmented (mobile) networks, where connectivity to centralized authentication entities and WoT keyservers is not available. Our approach enables a particular functionality in this scenario: The assessment of messages from previously unknown publishers. The demonstration will show a prototype running on Android devices.

## 2. DISASTER SCENARIO

Recently, ICN approaches are considered as a solution to enable communication after a disaster took place (e.g. a hurricane, earthquake, or tsunami) [6] [2]. In such a situation, it can be expected that parts of the communication infrastructure have broken down. The (formerly connected) network may be *fragmented* into several islands, e.g. due to failure of certain devices and communication links. Communication resources will be more limited than before the disaster, while at the same time it is important to efficiently distribute key

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s). Copyright is held by the author/owner(s).
*ICN'14,* September 24–26, 2014, Paris, France.
ACM 978-1-4503-3206-4/14/09.
http://dx.doi.org/10.1145/2660129.2660130.

disaster-related information (e.g. notifications from authorities, or critical rescue information to and among citizens) over the remaining functional parts of the communication infrastructure. One can assume that users (or rescue teams) can move among several of the fragmented network 'islands' over time, connecting each time to any functional network equipment in each 'visited' fragmented network. Given such a setting, decentralised authentication is challenging: In mobile networks, users are authenticated via central entities. Another challenge is the decentralised authentication of content retrieved from the network. Independent of the network being fixed or mobile, data origin authentication of content retrieved from the network is challenging when being 'offline', i.e. disconnected from servers of a security infrastructure such as a PKI [2].

Figure 1 [5] shows an example scenario of a mobile network after a disaster. Connectivity to the backbone or the Internet is broken, but certain parts of a mobile network infrastructure, e.g. base stations, are functional, forming small fragmented sub-networks. User $A$ is in a different fragment than user $X$. Rescue teams ($R$) are moving across different network fragments, and may transport messages from one disconnected sub-network to another one in a DTN[1]-like routing/forwarding fashion.

# 3. HIGH-LEVEL OVERVIEW OF SCHEME

We have proposed a detailed scheme for decentralised message authentication in ICN in a previous publication [5]. Here we summarize our scheme on a very high level; we refer the reader to our previous publication [5] for a detailed description and analysis of our scheme. Our scheme is based on a *Web-of-Trust (WoT)*. In particular, a so-called 'WoT file' (which can be retrieved from a WoT keyserver before the disaster takes place) is being used by terminals. This file contains the verified certificate graph for the whole WoT in a compressed, machine-readable format. Terminals thus have the complete trust relationships within the WoT at their disposal, in the from of a 'WoT-graph' stored in a file.

The binding between self-certifying ICN names and a Web-of-Trust is achieved as follows (see [5] for a detailed naming scheme and message flow): The WoT key-ID is equivalent to the self-certifying name part used in the ICN naming scheme. This ties the self-certifying name with the ID of the correct public key in the WoT, and thus transitively with the RWI in the WoT (e.g. an email address of a user). When information is received as a response to a given request ('Interest' in CCNx jargon) for a certain name (which in ICN usually represents the publisher of the name in some form), a *distributed Breadth First Search* ($dBFS$) algorithm is executed on the WoT-graph to find *certificate chains* between the initiator of the request and the publisher of the content. Depending on a *trust metric* (see Section 4 for some examples) that is applied on the result of the $dBFS$ algorithm, the information received is regarded as trustworthy or not by the initiator of the request.

# 4. DEMONSTRATION OUTLINE

The use case the demontration will show is *Assessing Warnings* (compare Fig. 1): A member of a mobile rescue team, $R$, is retrieving messages from citizens that publish warnings or other important information under a given name in a content-oriented architecture. $R$ is disconnected from any central server or authentication infrastructure (i.e. $R$ is 'offline'), so $R$ needs to assess the trustworthiness of messages from unknown parties (e.g. $X$, $Y$), in order to decide whether to react immediately on a given message, or which messages to forward to authorities at the next encounter of a new fragmented network. Note that the same use case occurs when $R$ is not a member of a rescue team but an average user: Still assessment of information retrieved which has been published by potentially unknown parties is necessary. The demonstration will show how our scheme actually performs—for addressing the use case described above—in a completely decentralised fashion, i.e. running solely on terminals without any help from infrastructure nodes. It will exemplify how how the computation of several trust metrics scales with increasing WoT sizes, and how the scheme actually performs on common smartphones/tablets (depending on WoT-size and concrete trust metric, which both can be selected by the user of the demo).

To evaluate our approach on realistic large-scale WoT-files, we developed a methodology to synthesize WoT-graphs of arbitrary size that maintain several key graph theoretic properties as prevalent in the PGP Web-of-Trust. We implemented this WoT-model in the JAVA-based *Graph-Theoretic Analysis Framework GTNA* [1], such that WoT-graphs with arbitrary size can be generated that conform to degree distribution, path length distribution, and other key graph-theoretic properties as found in existing small-size PGP-graphs. Also, we implemented a $dBFS$-algorithm in $GTNA$ for finding certificate chains on WoT-graphs. Furthermore, we implemented several trust metrics (a user-defined threshold for each metric decides whether a given WoT-node will be regarded as trustworthy or not): a) shortest certificate chain found, b) number of certificate chains found with maximum length, c) weighted certificate chain based on centrality-degree of intermediate nodes in the WoT-graph.

The demonstration will feature an Android-based terminal on which artificially-generated large-scale Web-of-Trust graphs will have been pre-loaded in the form of 'WoT files'. The terminal executes our implementation of the scheme on a given WoT-graph. In the demo, the user can choose among various trust metrics and parameters, as well as the WoT network size. Then, a publisher and retriever of information are randomly choosen from the WoT-graph; algorithm-execution, time, and other performance indicators are visualised to the user. The user can thus get a feeling of how the scheme actually performs (i.e. how much time it takes) on real devices depending on WoT-size and trust metric.

**Acknowledgment**: This work has been partially supported by the GreenICN project, a research project supported jointly by the European Commission under its 7th Framework Program (contract no. 608518) and the National Institute of Information and Communications Technology (NICT) in Japan (contract no. 167).

# 5. REFERENCES

[1] "Gtna - graph-theoretic network analyzer," website. [Online]. Available: https://www.p2p.tu-darmstadt.de/research/gtna/

[2] M. Arumaithurai, J. Seedorf, A. Tagami, K. Ramakrishnan, and N. B. Melazzi, "Using icn in disaster scenarios," Internet Engineering Task Force, Internet-Draft draft-seedorf-icn-disaster-02, June 2014, work in progress. [Online]. Available: http://tools.ietf.org/html/draft-seedorf-icn-disaster-02

[3] T. Aura, "Cryptographically generated addresses (cga)," in *Proc. of Information Security, 6th International Conference, ISC 2003*, ser. LNCS, Springer, Ed., no. 2851, October 2003, pp. 29–43.

[4] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker, "Naming in content-oriented architectures," in *Proceedings of the ACM SIGCOMM Workshop on Information-centric Networking*, 2011, pp. 1–6.

[5] J. Seedorf, D. Kutscher, and F. Schneider, "Decentralised binding of self-certifying names to real-world identities for assessment of third-party messages in fragmented mobile networks," in *2nd Workshop on Name Oriented Mobility (NOM)*, 2014.

[6] G. Tyson, E. Bodanese, J. Bigham, and A. Mauthe, "Beyond content delivery: Can icns help emergency scenarios?" *IEEE Network (to appear)*, 2014.

[1] Delay Tolerant Networking