NEXT GENERATION INTERNET

Open Call 4

Securing Content Delivery and Provenance (SECOND)
Deliverable 3: Experiment Results and Final Report

Authors	Nikos Fotiou, Yannis Thomas, Vasilis Kalos, George Xylomenos, Vasilios A. Siris, George C. Polyzos Mobile Multimedia Laboratory Department of Informatics School of Information Sciences and Technology Athens University of Economics and Business, Greece {fotiou,thomasi,kalos20,xgeorge,vsiris,polyzos}@aueb.gr In collaboration with Christos Papadopoulos, Spiros Thanasoulas Department of Computer Science The University of Memphis, USA {christos.papadopoulos,sthnslas}@memphis.edu
Due Date	September 15, 2022
Submission Date	September 14, 2022
Keywords	Decentralized Identifiers (DIDs), Public Key Infrastructure (PKI), ICN, NDN, mutable, immutable, content authenticity

Deliverable 3: Part I

Analysis, results, and wider impact

1 Abstract

SECOND extended the Named-Data Networking (NDN) implementation of the Information-Centric Networking (ICN) paradigm, using Decentralized Identifiers (DIDs) to support a self-sovereign, content authentication scheme, Verifiable Credentials (VCs) to support authorized network layer operations, and Zero-Knowledge Proofs (ZKPs) to support partial revelation of content. SECOND integrated DIDs and VCs into the core NDN functions, allowing it to secure content caching and forwarding, and enabled the binding of DIDs to human-readable content names, to simplify user interaction. The latter was made possible after closely cooperating with the NDN experts at UofM and co-designing a solution that does not require any modifications to the NDN codebase. The collaboration consisted of (at least) monthly video conferences and a visit from one of the members of the AUEB Team to the UofM. The UofM will exploit the DID-based identification and ZKP-based selective disclosure schemes developed by SECOND for their NSF-funded secure vehicular data project.

2 Project Vision

The *Securing Content Delivery and Provenance* (SECOND) project explored the full potential of *Self-Verifiable Content* (SVC) in *Named Data Networking* (NDN) [1], the most popular *Information-Centric Networking* (ICN) implementation [2]. SECOND exploited the *Decentralized Identifier* (DID) paradigm [3] for self-sovereign identities and, in particular, the *did:self* method [4] which was specified and implemented during the NGIatlantic.eu funded project SCN4NDN [5]. SECOND improved the trustworthiness of NGI architectures, giving users control of their data, decreasing the need for trusted intermediaries, enabling new security-sensitive applications, as well as enhancing users' privacy.

SECOND integrated SVC in many of the inter-networking functions of NDN, which, combined with a vertical ICN-based security management API:

- Improved the security and reliability of critical components for content delivery, such as caches and forwarders. SVC (a) prevents advertisement of "fake" content items, (b) allows controlled delegation of "content storage", and (c) enables new trust relationships among namespace "owners", content "producers", and content "storage providers".

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

- Improved SVC usability and content provenance, by supporting human-readable names through *Certificate-less Public Key Cryptography* (Certificate-less PKC). did:self (as most DID methods) uses public keys as DID identifiers, which are not human memorable. Certificate-less PKC is an "identity-based" encryption system that allows arbitrary strings to be used as public keys. However, as opposed to commonly used identity-based encryption systems, certificate-less PKC does not suffer from the so-called "key escrow" problem, i.e., there is no trusted entity that should generate all private keys; instead, each entity can securely generate (and keep secret) the private key that corresponds to an identity.

- Enhanced privacy, by allowing the retrieval of verifiable subsets of SVC using BBS+ digital signatures, which support *Zero-Knowledge Proofs* (ZKP). Using this approach, storage providers are able to hide portions of an SVC, without preventing content consumers from verifying its integrity. This allows fine-grained access control mechanisms that can prevent content consumers from accessing sensitive parts of the content, without losing the SVC property offered by the DIDs.

- Simplified security management, by leveraging the information-centric API of NDN. did:self is a "registry-less" DID method. Although this has many advantages, it creates challenges when it comes to revocation. Similarly, Certificate-less PKC requires the dissemination of some system-wide "parameters", as well as a name registration system. SECOND experimented with a solution that uses NDN itself to provide this functionality.

3 Details on participants (both EU and US)

This project was a joint effort between the Athens University of Economics and Business (AUEB) and the University of Memphis (UofM).

The **AUEB team** includes the following members:

George Xylomenos (M), Professor
Role Project Manager
George Xylomenos is a Professor at AUEB and a member of the Mobile Multimedia Laboratory (MMlab). He received his Diploma in Informatics from AUEB and M.Sc. and Ph.D. degrees from the University of California, San Diego. From 2009 to 2018 he was the director of Network Operations at AUEB, and from 2017 to 2020 he was the deputy rector for Finances, Planning and Development at AUEB. His current research interests include future Internet and Information-Centric Networking architectures and improving the performance of digital media applications and protocols over mobile and wireless networks. He has participated in the groundbreaking EU-funded projects PSIRP, PURSUIT, and POINT that

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

developed and implemented an ICN architecture and integrated it as an underlay for the Internet and recently in the SOFIE project on federated IoT with blockchains.

George C. Polyzos (M), Professor

Role Technical Manager

George C. Polyzos is leading the Mobile Multimedia Laboratory (MMlab) at AUEB, where he is Professor since 1999 and Director of the Graduate Program in Computer Science. Previously, he was Professor of Computer Science and Engineering at the University of California, San Diego (1988-1999), where he was co-director of the Computer Systems Laboratory, member of the Steering Committee of the Center for Wireless Communications and Senior Fellow of the San Diego Supercomputer Center. He received his Diploma in Electrical Engineering from the National Technical University in Athens, Greece and his MASc in Electrical Engineering and PhD in Computer Science from the University of Toronto, Canada. Under his leadership the MMlab has participated in a series of research projects funded by the European Commission, the European Space Agency, and Greece that co-developed Publish-Subscribe Internetworking, an Information-Centric Networking architecture, with project PURSUIT receiving the Future Internet Award. His current research interests focus on digital identity technologies and applications, (e.g., Decentralized Identifiers, Verifiable Credentials and their Selective Disclosure), the Internet-of-Things, security and privacy, Internet architecture and protocols, and Smart-Grid technology design and applications. He is currently leading MMlab's participation in H2020 project InterConnect on Smart-Grid interoperability and until recently SOFIE, investigating Distributed Ledger and Interledger Technologies, including smart contracts, for IoT systems federation and smart homes and energy grid evolution, focusing on openness, security, privacy, and business incentives. He was the founding chair of the Steering Committee of the ACM SIGCOMM conference on Information-Centric Networking and is now on the Steering Committee of the IFIP Wireless and Mobile Networking Conference. He has also been reviewer and panellist for the US NSF and the EC and reviewer for the California MICRO program, the Swiss National Science Foundation, the European Coordinated Research on Long-term Challenges, and the Greek General Secretariat of Research and Technology.

Vasilios A. Siris (M), Professor

Role Contributed to DID-related activities and the integration with NDN

Vasilios A. Siris is Professor at AUEB and a member of the Mobile Multimedia Laboratory (MMlab). Previously he was an Assistant Professor at the Department of Computer Science of the University of Crete (2002-2008) and a Research Associate at the Institute of Computer Science, Foundation for Research and Technology - Hellas / FORTH (1993-2015). His current research interests include resource management and traffic control in wired and wireless networks, exploitation of Distributed Ledger Technologies (DLTs) and blockchains for trusted communication with constrained and mobile devices in the Internet of Things, and architecture of future mobile terrestrial/satellite and pervasive communication systems. He

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

participated in the H2020 project SOFIE (Secure Open Federation for Internet Everywhere), where he was leading the architecture and framework evaluation.

Nikos Fotiou (M), PhD, Researcher
Role Led the DID-related tasks and security-related experiments design
Nikos Fotiou is a senior researcher with the MMlab/AUEB, where he completed his PhD in 2014 on "Information-Centric Networking: Security Requirements and Solutions." He received his MSc in Internetworking (2007) from the Royal Institute of Technology (KTH), ICT Dept., and the Diploma in ICSD Engineering (2005) from the University of the Aegean, Dept. of Information and Communications Systems Engin. He was a key MMlab researcher on projects PSIRP, PURSUIT, POINT, ϕSAT, I-CAN and others, and until recently led the contributions of the MMlab in H2020 SOFIE on security solutions based on decentralized identifiers and verifiable credentials. His current research interests include user privacy, access control mechanisms, and content integrity and provenance verification. He has co-authored 18 journal publications and more than 44 conference and workshop papers, with more than 3300 citations.

Yiannis Thomas (M), PhD, Researcher
Role Led NDN integration and network-related experiment design
Yannis Thomas is a postdoctoral researcher at the Department of Informatics of AUEB and member of the Mobile Multimedia Laboratory (MMlab). He received his Diploma in Informatics (2009), his MS in Information Systems (2012) and his PhD in Computer Science (2018) from the Department of Informatics of AUEB, Greece. He has contributed to a series of research projects funded by the European Commission (EC), the ESA, and Greece, such as the EC-funded projects "Publish Subscribe Internet Technology", "iP Over IcN-the betTer IP" and "Secure Open Federation for Internet Everywhere", and the ESA-funded project "The role of satellite in the future Internet". His research interests include multiflow transport protocols, congestion and flow control in the current Internet and Next Generation Networks, including Mobile Adhoc NETworks (MANETs) and heterogeneous Satellite-Terrestrial networks. He has co-authored more than 20 refereed articles in international journals, books, and conferences, including top-tier venues such as the IEEE INFOCOM and *IEEE/ACM Transactions on Networking*. He has also been a reviewer for international journals, such as the *ACM Transactions on Mobile Computing*, Elsevier *Computer Networks* and *Computer Communications*.

Vasilis Kalos (M), PhD student
Role Led activities and experiments related to ZKPs
Vasilis Kalos received his Diploma in Mathematics (2020) and his MS in Computer Science (2021). He participated in the ZeroTrustVC project of the Mobile Multimedia Laboratory (MMlab), on using Verifiable Credentials and OAuth for continuous authentication over HTTP. He is an active member of the Decentralized Identity

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

Foundation's applied crypto working group developing the BBS+ specification, in MATTR's team, a leading company in the SSI space. His research interests include applied cryptography, zero-knowledge proofs, practical (cryptographically secure) anonymous credentials systems and post quantum cryptography.

The **UofM team** is composed of the following members:

Christos Papadopoulos (M), Professor
Role Assisted in designing experiments for the NDN testbed and the UofM servers
Christos Papadopoulos received his PhD in 1999 from Washington University in St. Louis, MO. Before joining the Computer Science Department at the University of Memphis he was an assistant professor at the University of Southern California and a professor at Colorado State University. His research interests include network and cyber-physical systems security, global Internet measurements, information-centric networks and smart and autonomous systems. From 2018-20 he was a program manager at the Department of Homeland Security (DHS) Science and Technology directorate (S&T), where he managed projects on cyber-physical systems security, including industrial control systems, law enforcement and automotive cybersecurity. Dr. Papadopoulos was involved in research projects in excess of $10M and served as a principal investigator on projects funded by DHS, DARPA and the NSF. Recent projects address Internet-wide security problems such as Distributed Denial of Service (DDoS) attacks and detecting evasive Internet bots, analysis of global Internet routing, and applications of future Internet architectures in scientific domains such as climate and high-energy Physics through Named Data Networking (NDN). He is a senior member of the IEEE and has served on numerous ACM and IEEE conference program committees.

Spiros Thanasoulas (M), M.S., Software Engineer
Role Assisted in implementing experiments in the NDN testbed and extensions to NDN
Spiros Thanasoulas is a senior software engineer with the computer security lab at the University of Memphis. He holds a BSc in physics from the University of Crete, and an MSc in computer science from the University of Illinois Urbana-Champaign. In the past he has worked as a systems administrator for the Physics Dept. of the University of Crete (2001-2004) and a research assistant at FORTH (2005-2009), working, among other projects, on the MAPI flow tool. From (2014-2019) he worked as a research software engineer for the network security lab of Colorado State University. There he designed and developed BGPmon, an Internet scale BGP monitoring solution and high-speed network capture components for NetBrane, a DDoS detection and mitigation platform. Since 2019 he is associated as a Security Engineer with CENSUS Labs, a leading European cybersecurity services provider. He is interested in operating system interfaces mostly in BSD unix and Plan9. He is fluent in C, golang and scheme.

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

4 Results

SECOND performed the following experiments (the source code of the experiments and instructions for reproducing them can be found at https://github.com/mmlab-aueb/second):

4.1 Data authentication/verification using human readable DIDs and VCs

In this scenario, a content owner uses Certificate-less PKC to generate human readable DIDs used to protect content items. A human readable DID (e.g., "mmlab") is used as a content name prefix (e.g., "mmlab/document1"), and the DID-based mechanisms developed in our SCN4NDN project, are used to protect the corresponding content's integrity and authenticity. In this experiment we take advantage of the signing capabilities of Certificate-less PKC described in section 5.2 of [6]; the base64 encoding of a signature is 352 bytes, the generation of a signature in our VMs requires 4.9 ms, while the verification of a signature requires 6.8 ms.

Another extension to our SCN4NDN work explored with this experiment is an alternative mechanism for retrieving DID documents. In particular, the DID document that corresponds to the owner's DID is not included in the content item; instead, it is retrieved using legacy NDN operations. The information included in the DID document is used by the owner to issue an appropriate VC that authorizes a Producer application running in a VM attached to the testbed node at MMlab to provide (serve) the protected item to the NDN network. The same Producer application hosts a copy of the DID document for the content owner. This scenario demonstrates that due to the caching properties of NDN, DID documents are retrieved fast.

In particular, the scenario includes two Consumer applications, running in a VM attached to the testbed node of UofM and both requesting the same item. Upon retrieving the protected item, they request the DID document required for validating the included VC and metadata. It can be observed that the second Consumer retrieves the DID document much faster. This scenario is illustrated in Figure 1. As it can be seen, initially Consumer 1 receives the DID document directly from the Producer (Figure 1.A), but Consumer 2 receives a cached version of the DID document (Figure 1.B)

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020
Framework Programme of the European Union

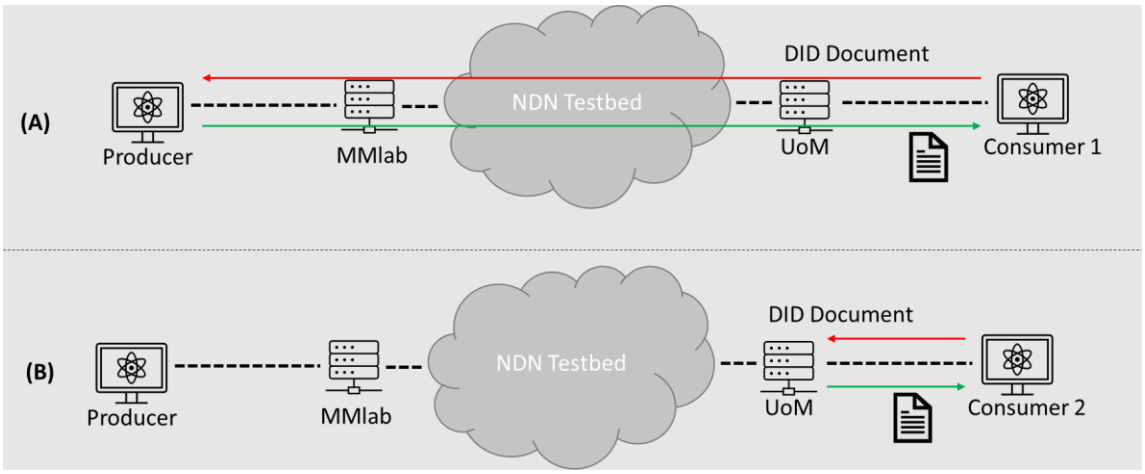

Figure 1 Certificate-less PKC setup

In our experiments, Consumer 1 receives the DID document in 197 ms, whereas Consumer 2 receives it almost instantly.

4.2 Partial content revelation using ZKPs

In this scenario, a content owner signs a JSON-encoded item using the BBS+ digital signature algorithm. This item represents a set of measurements from an IoT device. Then, a Producer application, running in a VM attached to a testbed node at MMlab, provides (serves) this item. A Consumer application, located in a VM attached to a testbed node at UofM, sends an Interest for a *subset* of these measurements by providing a "frame" in the *ApplicationParameters* option of the Interest packet header. The Interest packet is received by the Producer, which extracts the “frame”, “hides” the fields of the file not included in the frame, generates a ZKP for the new files, and sends the file back to the consumer.

Our experiment is illustrated in Figure 2. On the left part of the figure, the actual JSON encoded item can be seen. Then a Consumer sends an Interest packet that includes a frame. That frame specifies that the Consumer is only interested in the “owner” and “temperature” fields. The Producer hides from the item the fields not included in the provided frame and sends the corresponding response (bottom part of the figure).

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020
Framework Programme of the European Union

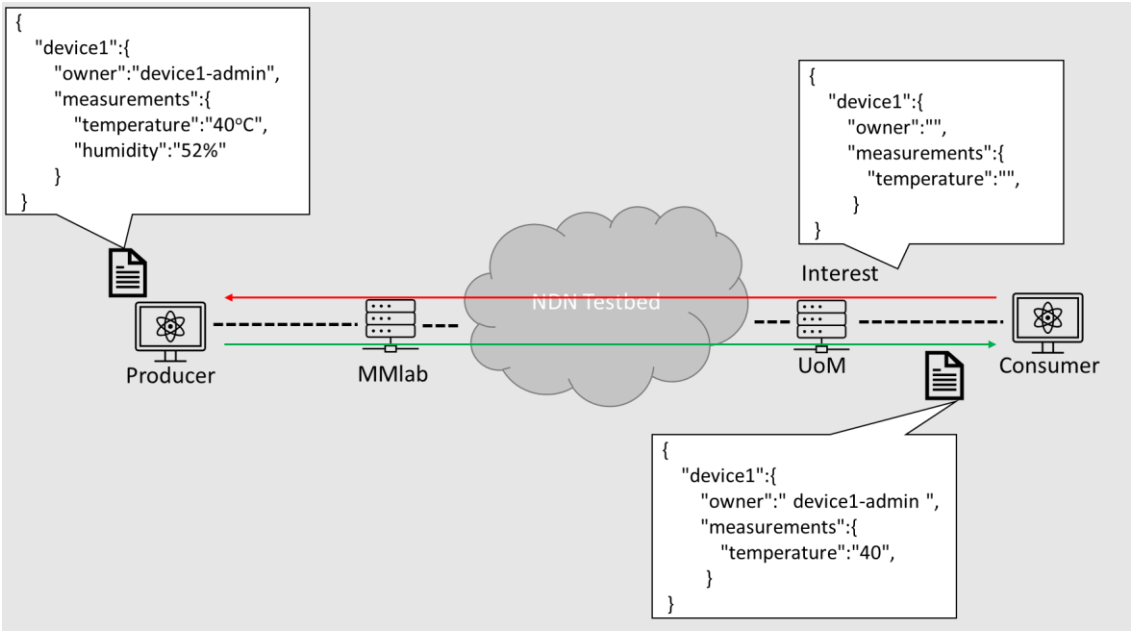

Figure 2 Partial content revelation setup

With our experiments we verified that ZKP generation latency depends on the number of hidden items (the more the hidden items the more time required to generate the ZKP) whereas the time to verify a ZKP is almost constant. Figure 3 illustrates the measurements performed in our VMs.

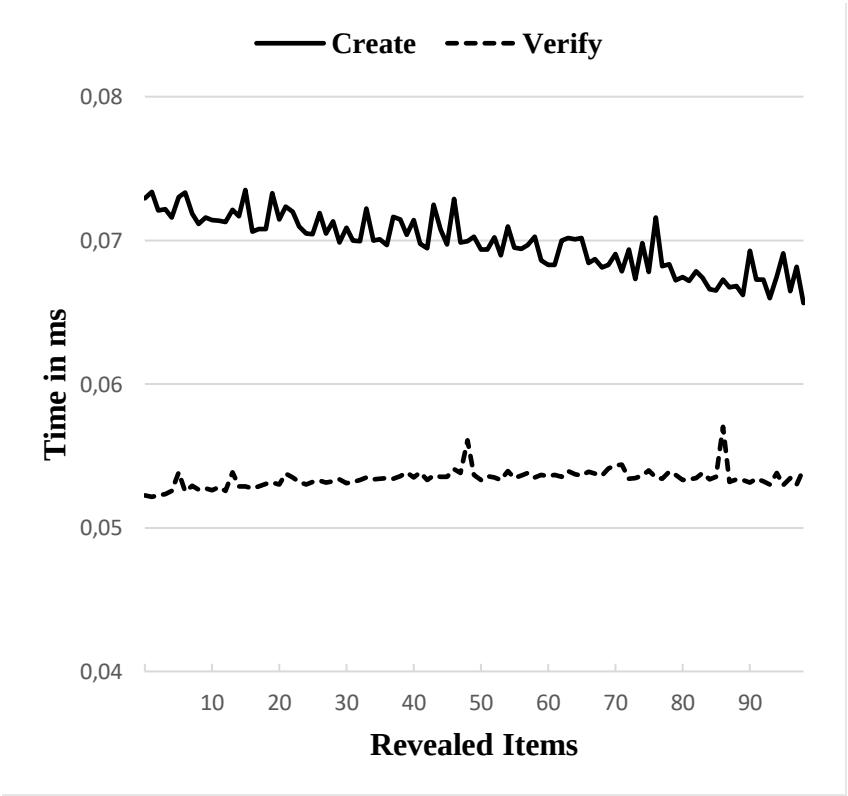

Figure 3 ZKP generation and verification time

Co-funded by the Horizon 2020
Framework Programme of the European Union

4.3 Authorized prefix advertisement

In this scenario, we present how the DID/VC-based authorization mechanism that we developed was integrated into NDN's core functionality. In particular, we demonstrate how this mechanism can be used to allow only authorized nodes to advertise a prefix. This scenario considers the following setup. An application acts as a *Gateway* to the NDN testbed. All Producers interact with the NDN testbed through this Gateway. Producers send advertisements to the Gateway, as well as a VC that proves that they are authorized to advertise the specific prefix. If the VC is valid, the Gateway forwards the advertisement to the NDN testbed. An Interest for an item advertised in this manner, will flow to the Producer through the Gateway.

In this experiment, the Gateway and the Producer applications are located in a VM attached to a testbed node at MMlab, while the Consumer application is located in a VM attached to a testbed node at UofM, as illustrated in Figure 4.

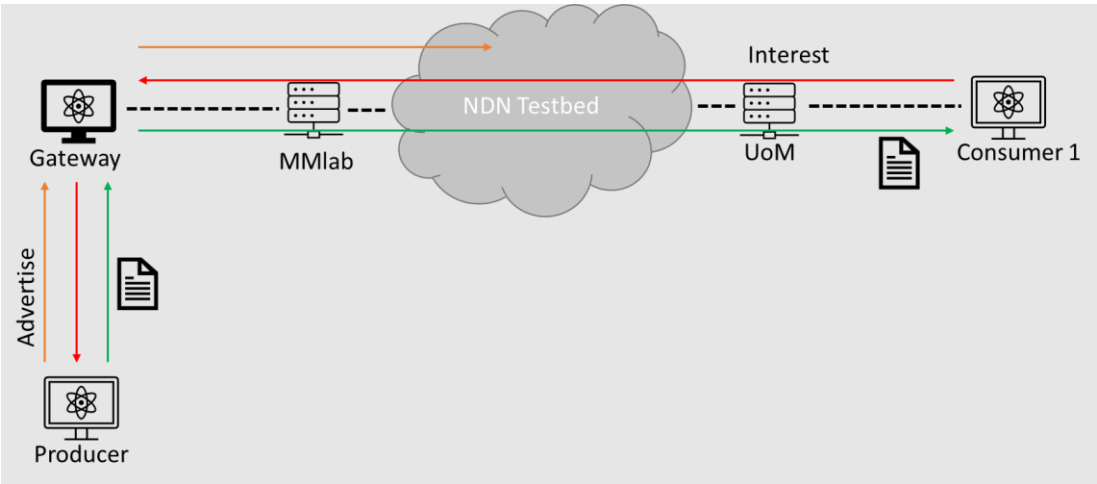

Figure 4 Authorized advertisement Setup

Because all operations are implemented using native NDN, the NDN daemon running on the Gateway will cache the items received from the Producer. Therefore, subsequent Interests for the same item will be responded to by the Gateway directly.

4.4 Discussion and Analysis on Results

The results obtained show that the proposed solutions are valid and can be integrated into NDN (and ICN in general). All the goals set in the proposal have been achieved, that is, use of Certificate-less PKC to securely bind names to content, use of ZKPs for partial content revelation and full integration of our scheme into NDN, including exploitation of caching, without changing the code running in the NDN testbed.

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

Our experiments helped us discover two issues. The first issue is related to the caching of DID documents. In NDN, two items that have the same name are considered identical. In our experiments we used a "well-defined" name for storing DID documents (in the form of "/ndn/<node>/<DID>/document"). Then, we emulated an attack scenario in which the content owner rotates its key, thus producing a new DID document. Let "DocumentOld" be the old DID document and "DocumentNew" the updated DID document. Assume now that the following sequence of events takes place:

1. A Consumer requests and receives a protected item,
2. The Consumer requests the corresponding DID document and receives from a cache "DocumentOld,"
3. Since this is the deprecated document, the signatures in the protected item cannot be verified, hence the Consumer sends a new Interest indicating that it wants a "fresh" version of the DID document,
4. The producer responds with "DocumentNew", which can be used for verifying the signatures in the protected item.

It was expected that after step 4, the cache would replace "DocumentOld" with "DocumentNew," but this did not happen because, from the cache's perspective, since these two items have the same name, they are identical. As a result, subsequent requests for the DID document result in receiving "DocumentOld" from the cache. A workaround for fixing this issue is to include in the metadata of a content item the "versions" of the DID documents that should be used for validating it. Further solutions for this issue will be investigated as future work.

The second issue we discovered is related to how NDN handles the information included in the *ApplicationParameters* option of an Interest packet. In particular, NDN transparently calculates a hash of that field and appends it to the name of the requested content item. For example, an Interest message for "/ndn/document1" that also includes some *ApplicationParameters,* from the network perspective appears to be an Interest message for "/ndn/document1/<hash(ApplicationParameters)>". Therefore, in our second scenario, when two Consumer applications request the same "frame" of an item and include only the frame in the *ApplicationParameters* option, they will send the same Interest message, therefore the second Consumer may receive the requested item from a cache. However, if the Consumers also include their "authorization VC," the Interest messages will always be different. This happens because every authorization VC includes a Consumer-owned public key, therefore authorization VCs have to be different from each other. After discussions with our US-based partners, we concluded that this issue cannot be fixed without modifications to the NDN API.

A declared goal of this project was the integration of our security mechanisms into the core functions of NDN. Our initial plan was to modify NDN's code in order to integrate the desired functionality. Nevertheless, after discussions with UofM it was realised that those core functions are implemented using the same primitives that higher layer API uses, i.e., Interest

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020
Framework Programme of the European Union

and Data packets. Based on this observation, both partners co-designed a solution that achieves protection of "Advertisement" messages without modifying NDN's code. We believe that this is a significant achievement, since it creates opportunities for new security solutions that can be easily tested and deployed.

5 Present and Foreseen TRL

The project developed and enhanced various software modules. The following table provides information about the TRL of each module. In particular, it presents the TRL of each module before the beginning of the project, its current TRL, as well as its foreseen TRL one year after the completion of the project.

Module	Repository	Initial TRL	Present TRL	Foreseen TRL
did:self py Implementation	link	5	5	7 (did:self will be included in operational software developed by AUEB/MMlab members)
ZKP toolkit	link	0	4	5 (The toolkit is used in ongoing projects at AUEB/MMlab and will be demonstrated in relevant environments)
CPKC	Now is part of link	0	4	4 (The Charm-Crypro library is under maintenance and we do not foresee advancing the TRL of this particular module in the next year)
NDN Gateway	link	0	4	5 (The project team is preparing a publication about this approach, which we anticipate will result in further exploration of our software in relevant environments)

6 Exploitation, Dissemination and Communication Status

The project outcomes are expected to be of interest to both the Decentralized Credentials and Information-Centric Networking communities. For this reason, our exploitation, dissemination, and communication plan targeted both communities.

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

Project outcomes are reported on the project website (https://mm.aueb.gr/projects/second), which will also disseminate the code, papers and presentation made as part of the project. In addition, all software implementations are freely available in GitHub.

Project members participate in the W3C Credentials Community Group (W3C-CCG) [7], as well as in the Decentralized Identity Foundation (DIF) [8]. All DID-related outcomes will be presented to both groups.

Furthermore, project members participate in IETF's Information-Centric Networking research group (ICNRG) [9]. We presented the ZKP-based solution for partial content revelation developed as part of the SECOND project at the joint ICNRG and COINRG (Computing in the Network Research Group) at IETF-114 [10]. We have also established links with the NDN developer community and we plan to present our work in the periodic NFD seminars, and possibly at the NDNcomm yearly community meeting (scheduled after the end of the project). During the testing setup stage, we identified some bugs in the NDN certificate issuance process, and we assisted the NDN testbed team in fixing them, which helped our project gain visibility in the NDN area.

We already presented a paper at the IFIP SEC 2022 conference [11] which was prepared along with the proposal, on the subject of using VCs for selective disclosure. We also got a paper accepted to the GIIS 2022 conference [12], describing our ZKP-based solution for partial content revelation. Project members were also invited to participate in a panel at the ACM ICN 2022 conference [13]. We have under preparation another conference paper presenting our approach to securing NDN routing. Following these conference paper submissions, the project will target a submission to a high-quality journal (e.g., Elsevier's Computer Networks).

7 Impacts

With respect to the NGI initiative, our project is making an impact in the following areas:

- Enhanced EU – US cooperation in Next Generation Internet, including policy cooperation.

Beyond ICN, and ICT research in general, our project aimed to be a starting point for better EU-US relations in science and technology. AUEB and UofM have already established a fruitful relationship during the SCN4NDN project, which became more productive during SECOND: UofM is working on ICN for vehicular applications (see below), where partial content revelation (as developed by SECOND) is extremely useful; this was one of the main points discussed during the research visit of Prof. Siris to UofM. In addition, the ties established between AUEB and the (mostly US based) NDN testbed team allowed us to collaborate on solving the issues that we found with the certificate issuance process for NDN nodes. Finally, our experiment monitoring tool (see D2) will be made available to other NDN testbed users, assisting them in automating their own experiments.

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020
Framework Programme of the European Union

- Reinforced collaboration and increased synergies between the EU Next Generation Internet and the corresponding NSF programmes.

Our project combines EU-based and US-based researchers and resources to experiment with networking architecture and components that are of interest to both the Next Generation Internet and the corresponding NSF programmes. For instance, our did:self method is applicable to a number of emerging authentication and authorization standards. Furthermore, our DID-based content authentication mechanism can be applied in other contexts. UofM has recently been awarded an NSF-funded (award #2213733) secure in-vehicle data collection and distribution using ICN, called Open Community Platform for Sharing Vehicle Telematics Data for Research and Innovation, with the aim of building a Platform for Innovative use of Vehicle Open Telematics (PIVOT) [14]. This is a great match with SECOND, both in the authentication area, where DIDs can be used, and in the selective disclosure of vehicular data, where the ZKP approach can be employed. Possible collaborations on future research projects were discussed during the visit of Prof. Siris to UofM. We also established links with the Inter-Planetary File System (IPFS) team and collaborated with them in combining DIDs with IPFS [15].

- Developing interoperable solutions and joint demonstrators, contributions to standards

Our project was a showcase of the merger of two emerging standards, managed by different standardization bodies. On the one hand, DIDs are primarily pursued by the W3C. On the other hand, ICN standards are mainly developed under the umbrella of the IETF. Both standardization efforts involve partners from academia and industry. Beyond the demonstration of the joint standards, the project aims to inspire new activities in the respective standardization bodies. We are very actively pushing DIDs to the ICN community, with multiple workshop and conference submissions as part of the project, as well as a recent presentation to the ICNRG WG of the IRTF, focusing on routing security and partial content revelation. As part of SECOND, we implemented Certificate-less PKC for the Charm-Crypto cryptographic library. After making a pull request to the library's github repository that includes our contribution[1], it has now been merged to the "dev" branch, which is available to all developers using the library.

- An EU - US ecosystem of top researchers, hi-tech start-ups / SMEs and Internet-related communities collaborating on the evolution of the Internet

We envisioned this project to be not a mere collaboration between two ICN pioneers but to also establish and maintain a permanent link between EU-US ICT research based on the Future Internet ICN approach. EU ICN research efforts are more human-centric, focusing mostly on

[1] https://github.com/JHUISI/charm/pull/286

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

security and trust, self-sovereignty, and distributed data governance. US efforts on the other hand prioritize deployment and real-world exploitation. The AUEB team is focusing on solutions for ICN security and privacy (both in terms of content and access patterns), which we are aiming to integrate with the UofM approach in exploiting ICN for vehicular networks.

By expanding the scope of SVC and the capabilities it offers in the SECOND project, such as supporting human readable content names and selective disclosure of content, as well as embedding the did:self mechanisms inside the core NDN implementation, we are making concrete progress in offering new abilities to NDN, thus making it more attractive for standardization. The workshop and conference submissions describing these advances, as well as their presentation to the ICNRG WG of the IRTF, served to create a momentum behind creating Internet Drafts. A second goal is to push this work to the W3C *Credentials Community Group* (CCG) and the *Decentralized Identity Foundation* (DIF), where technology companies, as well as policy makers from both EU and US participate, as case studies of practical uses of the DID and SVC concepts.

8 Conclusion and Future Work

SECOND explored the use of Decentralized Identifiers (DIDs), Verifiable Credentials (VCs) and Zero-Knowledge Proofs (ZKPs) for improving the security and privacy of Named Data Networking (NDN), the most popular Information-Centric Networking (ICN) implementation. Through experimentation in the NDN testbed, we validate our approach, and we discovered new issues. Starting from our previous NGIAtlantic.eu funded project SCN4NDN, SECOND was able to produce more results and achieve a bigger impact.

With SECOND we leveraged Certificate-less Certificate-less PKC and we implemented human readable DIDs, providing an improved user experience, compared to SCN4NDN that used public keys as DIDs. Additionally, we leveraged NDN's ICN functionality to disseminate DID documents, which resulted in smaller packets and improved resistance to key breaches. Furthermore, we managed to use this functionality to protect NDN's core functions without modifying the NDN code and/or its API. Finally, we experimented with a novel ZKP-based mechanism that allows selective content retrieval, again without modifying the NDN code and/or its API.

In SECOND the US-based partner had a larger contribution compared to SCN4NDN, as in addition to facilitating access to the NDN testbed, it co-designed the approach for using the developed security solutions to protect NDN advertisements. This is a significant achievement which provides a solid and realistic solution to a big problem of NDN, which is "content pollution". The research visit to UofM also helped us work on future collaborative projects.

SECOND produced two accepted scientific publications and some of the project results were presented in an IRTF meeting. Furthermore, in addition to the code made available to MMlab's

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020
Framework Programme of the European Union

public github repository, SECOND contributed its implementation of Certificate-less PKC to Charm-Crypto cryptographic library. Finally, project outcomes are used in related projects of both partners.

The project team prepares an additional scientific publication for a conference and a submission to a journal encompassing the entire project's results. Furthermore, it will further explore the possibilities discovered during the SECOND experiments, including improved revocation mechanisms and new in-network security solutions.

9 References

[1] V. Jacobson, D.K. Smetters, J.D. Thornton, M.F. Plass, N.H. Briggs, R.L. Braynard, "Networking Named Content," Proc. ACM CoNEXT 2009, Rome, Italy, December 2009

[2] G. Xylomenos, C.N. Ververidis, V.A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K.V. Katsaros, G.C. Polyzos, "A Survey of Information-Centric Networking Research," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1024-1049, 2014.

[3] W3C Credentials Community Group, "A primer for decentralized identifiers," 2019; available at https://w3c-ccg.github.io/did-primer/

[4] Mobile Multimedia Laboratory, "Did:self method specification," available at https://github.com/mmlab-aueb/did-self

[5] Mobile Multimedia Laboratory, "The SCN4NDN project," available at https://mm.aueb.gr/scn4ndn/

[6] S. S. Al-Riyami, K. G. Paterson, "Certificateless Public Key Cryptography," Lecture Notes in Computer Science, pp. 452 – 473, 2003

[7] W3C, "W3C Credentials Community Group Home Page," available at https://www.w3.org/community/credentials/

[8] DIF, "Decentralized Identity Foundation Home Page," available at https://identity.foundation

[9] IETF, "Information-Centric Networking Research Group (icnrg) charter," available at https://datatracker.ietf.org/rg/icnrg/about/

[10] IETF, "Agenda for the joint ICNR & COINRG Meeting at IETF-114," available at https://datatracker.ietf.org/meeting/114/materials/agenda-114-icnrg-03

[11] V. Kalos, G.C. Polyzos, "Requirements and Secure Serialization for Selective Disclosure Verifiable Credentials," Proc. 37th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC), Copenhagen, DK, June 2022.

[12] N. Fotiou, V. Kalos, Y. Thomas, G. Xylomenos, V.A. Siris, G.C. Polyzos, "Selctive Content Disclosure using Zero-Knowledge Proofs," Proc. 2022 Global Information Infrastructure and Networking Symposium (GIIS), Argostoli, GR, September 2022.

[13] ACM ICN 2022 Conference Program, available at https://conferences.sigcomm.org/acm-icn/2022/program.html

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union

[14] University of Memphis, Colorado State University, Stanford Research Institute and Geotab, "PIVOT Project Home Page," available at https://pivot-auto.org/

[15]IPFS, "The InterPlanetary File System Home Page," available at https://ipfs.io

10 Glossary

AUEB	Athens University of Economics and Business (Coordinating partner)
CA	Certificate Authority
COINRG	Computing in the Network Research Group (of the IRTF)
DID	Decentralized Identifier
DIF	Decentralized Identity Foundation
IBE	Identity-Based Encryption
ICN	Information-Centric Networking
ICNRG	Information-Centric Networking Research Group (of the IRTF)
IPFS	InterPlanetary File System
NDN	Named Data Networking
NFD	Named Data Networking Forwarding Daemon
PIVOT	Platform for Innovative use of Vehicle Open Telematics
PKC	Public Key Cryptography
PKG	Private Key Generator
SSI	Self-Sovereign Identity
SVC	Self-Verifiable Content
UofM	University of Memphis (US-based partner)
VC	Verifiable Credential
W3C-CCG	W3C Credentials Community Group
ZKP	Zero-Knowledge Proof

© 2020-2022 NGIatlantic.eu

Co-funded by the Horizon 2020 Framework Programme of the European Union