

## ISCC 2022 Tutorial Proposal

### **Self-Sovereign Identity (SSI), Decentralized Identifiers, and Verifiable Credentials** with applications to Access Control, Web Services, the Internet of Things, and Smart Cities

*Nikos Fotiou, George C. Polyzos, Vasilios A. Siris*  
Athens University of Economics and Business

April 30th, 2022

Half-day tutorial proposal (3 hours) related to the emerging topics:

- Secure computing and secure architectures
- Smart cities and IoT

#### **Abstract:**

Self-Sovereign Identity (SSI) is a concept that enables individuals or organization to have sole ownership of their identity and control how their personal data is shared and used. SSI allows entities to prove control of one or more identifiers without an intermediary and provides the flexibility for each entity to control which information or claims are revealed to third parties. The importance of providing citizens full control of their data and the decision of which data to disclose is a main objective of the eIDAS 2021 amendment (also referred to as eIDAS 2.0). The vulnerabilities of existing procedures in handling personal data are highlighted by unauthorized access to sensitive data due to data breaches. At the same time, it is becoming increasingly challenging for companies to ensure secure and trusted digital interaction with customers and manage employee authorizations, while there is an increasing need for inter-domain trusted communication and cross-organization authorization. SSI technology, including decentralized identifiers and Verifiable Credentials, can address the above issues in order to unleash tremendous economic potential improving the security, trust, and efficiency while also supporting the privacy of user data.

#### **Objectives:**

The objectives of the tutorial are to familiarize the attendees with these technologies, create an appreciation for Self-Sovereignty, promote improved privacy solutions and strict security and stress the importance of all these for the IoT, Smart Cities and the digital transformation in general, where much critical information will be available in digital form, interconnected, but somewhat unseen or forgotten by the owners or its subjects and thus usable, consistent, and potentially automated access control should be provided.

#### **Topics:**

See the outline below about topics. Motivation is in the abstract above. Timeliness is excellent! Most of these technologies are maturing now and are considered for standardization or adoption—e.g., the new eIDAS 2.0 recommendation is recommending the use of Self-Sovereign Identity technologies and digital wallets kept and controlled by citizens.

**Audience:**

Scientists, researchers, and engineers in the general area of ICT seeking to obtain a concise knowledge of the SSI concept, its underlying tools and mechanisms, and how they can be applied to and benefit interactions, transactions, and procedures in a range of application domains such as the Internet of Things, Smart Cities, access to Web Services, and Zero Trust Architectures. No prior knowledge of security or authentication/authorization mechanisms is necessary.

**Virtual presentation:**

The tutorial is proposed primarily as a virtual presentation, so that all 3 authors participate and share the delivery of the tutorial. Dr. Polyzos will most probably attend the conference and if it can be arranged and is convenient could be on location and deliver his parts in mixed mode, i.e., on location and through virtual presentation and also be back-up for.

**Experience of the speakers:**

The speakers have significant experience in presentations and participation in SSI-related standardization groups and relevant presentations. Some of the presentations were at a high-level, targeting a wider audience with no security/privacy background.

- “Using OAuth 2.0 for VC issuance,” Nikos Fotiou, W3C Credentials Community Group, 17/05/2022.
- “Continuous authorization over http using verifiable credentials & OAuth 2.0,” Nikos Fotiou, DIFCon Virtual F2F, Decentralized Identity Foundation, 24/02/2022.
- “Managing The Lifecycle of Verifiable Credentials using OAuth 2.0,” Nikos Fotiou, OAuth Security Workshop, 30/11 & 1/12/2021.
- “Access Control for WoT using VCs”, Nikos Fotiou, 22nd Vienna Digital Identity Meetup, 22/03/2021.
- “Decentralized Identifiers and Verifiable Credentials in SOFIE with applications in aviation,” George C. Polyzos, 3rd CHARIOT EU Project workshop, 22/10/2020.
- “Using Verifiable Credentials in IoT services,” Nikos Fotiou, joint W3C Web of Things (WoT) Interest Group and IRTF Thing-to-Thing Research Group (T2TRG) Virtual F2F meeting, 20-22/6/2020.
- “Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices,” Vasilios A. Siris, Decentralized Operation and Security in the IoT Space Workshop, cyberwatching.eu, 18/06/2020.
- Participation in W3C Credentials Community group and contribution to the Decentralized Identifiers (DIDs) v1.0 specification, N. Fotiou, 2020.
- Participation in the discussions on the IETF Internet-Draft "OAuth 2.0 Demonstration of Proof-of-Possession at the Application Layer (DPoP)", draft-fett-oauth-dpop-04, Nikos Fotiou, 2019 Q4/2020 Q1.
- Participation in a (pre-standardisation) meeting of the IRTF Decentralized Internet Infrastructure (DIN) Research Group (<https://irtf.org/dinrg>), George C. Polyzos, 17/02/2018.

Additionally, Nikos Fotiou and George C. Polyzos gave a well-attended tutorial (after an open call for tutorials and evaluation/selection) to the 1st ACM SIGCOMM ICN in 2014 to an audience with full ICN background and potentially limited security background:

- N. Fotiou and G.C. Polyzos, “[ICN Privacy and Name based Security](#),” Proc. 1st ACM SIGCOMM international conference on Information-Centric Networking (ICN '14), Paris, France, September 2014 (abstract of tutorial).

Furthermore, all authors of this proposal were co-authors of a widely cited survey paper [1] and are co-authors of a number of security and privacy papers that are listed below.

### **Tentative outline and schedule:**

Part 1 – Motivation and Challenges, duration: 45 minutes, presenter: George C. Polyzos

- Identity and Digital Identity
- Authentication, Authorization and Access Control
- Interoperability and cross-domain trusted communication
- The Evolution of Identity: Centralized, Federated, User-centric, and Self-Sovereign

Part 2 – SSI principles, Decentralized Identifiers, and Verifiable Credentials, duration: 1 hour and 30 minutes, presenter: Nikos Fotiou

- Self-Sovereign Identity (SSI) principles
- Decentralized Identifiers and W3C’s DID specification
- W3C Verifiable Credentials (VC) and VC issuance

Part 3 – Benefits and Applications, duration: 45 minutes, Presenter: Vasilios A. Siris

- Zero Trust Architectures
- Applications to web service access and cross-organization authorization
- Applications to authorization and delegation in the Internet of Things
- Applications to device access and data sharing in Smart Cities

### **About the Presenters:**

Dr. **Nikos Fotiou** is a post-doctoral researcher at the Mobile Multimedia Laboratory (MMLab), AUEB. Dr. Fotiou received his Diploma in Information Systems Engineering from the University of the Aegean, Samos, Greece, his M.Sc. in Internetworking from KTH, Stockholm, Sweden, and his Ph.D. in Computer Science from AUEB, Athens, Greece. His Ph.D. dissertation investigated security requirements and solutions for ICN architectures. His paper “Access Control Enforcement Delegation for Information-Centric Networking Architectures,” received the best paper award at the 2012 SIGCOMM ICN workshop. He is a contributor to the Charm-Crypto, cryptographic library. Dr. Fotiou is co-author of more than 30 papers, related to ICN architectures, security aspects of ICN, user privacy in ICN, access control, integrity and provenance verification mechanisms, as well as applications of ICN in the IoT. Dr. Fotiou has participated in many security and privacy related research projects, including: ZeroTrustVC (Enabling Zero Trust architectures using OAuth2.0 and Verifiable Credentials, eSSIF Labs), SECOND (Securing Content Delivery and Provenance, NGI Atlantic), SelectShare (Selective IoT data sharing, NGI DAPSI), and SOFIE (Secure Open Federation for Internet Everywhere, H2020). Dr. Fotiou has presented tutorials on ICN and its security aspects, during the EU FP7 Euro-NF summer school on ICN, the I-CAN Ph.D. course on ICN,

and the 2014 ACM SIGCOMM ICN conference. A full CV, including many security and privacy publications is available here: <http://pages.cs.aueb.gr/~fotiou/CVe.pdf>

Dr. **George C. Polyzos**, Professor of Computer Science at AUEB, founded and is leading the Mobile Multimedia Laboratory (MMLab). Previously, he was Professor of Computer Science and Engineering at the University of California, San Diego, 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. Prof. Polyzos and the MMLab participated in the EU FP7 projects PSIRP (“Publish-Subscribe Internet Routing Paradigm”) and PURSUIT (“Publish-Subscribe Internet Technology,” 2013 Future Internet Award, Dublin, Ireland 10 May 2013) that developed the Information-Centric Networking (ICN) Publish-Subscribe Internet (PSI) architecture, and co-authored a comprehensive and highly cited survey article on ICN. Prof. Polyzos was also an organizer of the EIFFEL (“Evolved Internet Future For European Leadership”) Think Tank, on the Steering Board of the Euro-NF Network of Excellence and head of its “Socio-Economic Aspects” and “Trust, Privacy and Security” joint research activities. His current and recent research projects include EU H2020 InterConnect (Interoperable Solutions Connecting Smart Homes, Buildings and Grids), ZeroTrustVC (Enabling Zero Trust architectures using OAuth2.0 and Verifiable Credentials, eSSIF Labs), SECOND (Securing Content Delivery and Provenance, NGI Atlantic), SelectShare (Selective IoT data sharing, NGI DAPSI), and H2020 SOFIE (Secure Open Federation for Internet Everywhere).

He has chaired the Steering Committee of the ACM SIGCOMM conference on Information-Centric Networking and was TPC Co-Chair for the ACM SIGCOMM ICN workshop. Dr. Polyzos received his Diploma in EE from the National Technical University, Athens, Greece and his M.A.Sc. in EE and Ph.D. in CS from the University of Toronto. He has published more than 250 refereed papers with more than 11.000 citations (h-index = 46). He has also advised 16 PhDs (8@UCSD, 8@AUEB), most having now academic or industrial positions in the US or Europe. Dr. Polyzos has been reviewer or panelist for many research funding agencies, including the European Commission, the US NSF, the California MICRO program, the Swiss NSF, the European ERA-Net, and the Greek GSRT; he has also been on the editorial board and guest editor for scientific journals, on the program committees of many conferences and workshops and at present he is also on the Steering Committee of the Wireless and Mobile Networking Conference, WG 6.8, IFIP TC6. He has also served on the IEEE Internet Award Committee (2008-2011) and many PhD committees of universities in Europe and the US and has given invited talks at many universities and events. His current research interests include Internet architecture and protocols, ubiquitous computing, the Internet of Things, and security and privacy. A full recent CV, including security and privacy publications, is available here: <http://niovi.aueb.gr/~gcp/CV-EN.pdf>

Dr. **Vasilios A. Siris**, Professor at the Department of Informatics of AUEB and MMLab member. 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 (1993-2011). He has been a Visiting Researcher at the Statistics Laboratory, University of Cambridge, UK (spring 2001), BT Labs, Ipswich, UK (summer 2001 and 2006), and University of Bern, Switzerland (summer 2012). His research interests include secure and trusted communication in the IoT, SSI and decentralized identifier technologies, and context-aware resource management in

mobile networks. He has published more than 100 refereed articles with over 5900 citations in Google Scholar. His current and recent research projects include EU H2020 InterConnect (Interoperable Solutions Connecting Smart Homes, Buildings and Grids), ZeroTrustVC (Enabling Zero Trust architectures using OAuth2.0 and Verifiable Credentials, eSSIF Labs), SECOND (Securing Content Delivery and Provenance, NGI Atlantic), SelectShare (Selective IoT data sharing, NGI DAPSI), and H2020 SOFIE (Secure Open Federation for Internet Everywhere). He has presented a webinar on “Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices,” in the Decentralized Operation and Security in the IoT Space Workshop, cyberwatching.eu, June 2020. He has one International and two national (Greek) patents related to wireless/mobile network management. A full recent CV, including security and privacy publications, is available here: <http://www2.aueb.gr/users/vsiris/>

### **Related Publications by the Proposers**

1. 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 and Tutorials, vol. 16, no. 2, pp. 1024-1049, 2014.
2. N. Fotiou, G.F. Marias, G.C. Polyzos, “Access Control Enforcement Delegation for Information-Centric Networking Architectures,” ACM SIGCOMM Computer Communication Review, vol. 42, no. 4, pp. 497-502, October 2012 (selected for journal publication as best paper of the 2012 ACM SIGCOMM workshop on ‘Information-Centric Networking’).
3. N. Fotiou, A. Machas, G.C. Polyzos, G. Xylomenos, “Access control as a service for the Cloud,” Journal of Internet Services and Applications, Springer, vol. 6, no. 1, June 2015.
4. N. Fotiou and G.C. Polyzos, “Decentralized Name-based Security for Content Distribution using Blockchains,” Proc. Workshop on Multimedia Streaming in Information-/Content-Centric Networks (MuSIC), in conjunction with IEEE INFOCOM, San Francisco, CA, USA, April 2016.
5. N. Fotiou and G.C. Polyzos, “Securing Content Sharing over ICN,” Proc. 3<sup>rd</sup> ACM Conference on Information-Centric Networking (ICN’16), Kyoto, Japan, pp. 176-185, September 2016 (<http://dx.doi.org/10.1145/2984356.2984376>).
6. N. Fotiou, T. Kotsonis, G. Marias, G.C. Polyzos, “Access Control for the Internet of Things,” Proc. International Workshop on Secure Internet of Things (SIoT 2016), in conjunction with the European Symposium on Research in Computer Security (ESORICS 2016), Heraklion, Greece, September 2016.
7. G.C. Polyzos and N. Fotiou, “Blockchain-assisted Information Distribution for the Internet of Things,” Proc. 4<sup>th</sup> International Workshop on Information Integration in Cyber Physical Systems (IICPS) in conjunction with the 18th IEEE International Conference on Information Reuse and Integration, San Diego, CA, USA, August 2017.
8. N. Fotiou and G.C. Polyzos, “Smart Contracts for the Internet of Things: Opportunities and Challenges,” Proc. European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia, June 2018.
9. N. Fotiou and G.C. Polyzos, “Authentication and Authorization for Interoperable IoT Architectures,” Proc. ESORICS Workshop on Emerging Technologies for Authorization and Authentication (ETAA), Barcelona, Spain, September 2018. Published in:

- Emerging Technologies for Authorization and Authentication (ETAA 2018), A. Saracino and P. Mori (eds), Lecture Notes in Computer Science, vol. 11263. Springer, ([https://doi.org/10.1007/978-3-030-04372-8\\_1](https://doi.org/10.1007/978-3-030-04372-8_1)), November 2018.
10. N. Fotiou, V.A. Siris, G.C. Polyzos, "Interacting with the Internet of Things using Smart Contracts and Blockchain Technologies," Proc. 11th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS), Melbourne, Australia, December 2018.
  11. N. Fotiou, V.A. Siris, S. Voulgaris, G.C. Polyzos, D. Lagutin, "Bridging the Cyber and Physical Worlds using Blockchains and Smart Contracts," Proc. Workshop on Decentralized IoT Systems and Security (DISS) in conjunction with the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2019.
  12. V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, "OAuth 2.0 Meets Blockchain for Authorization in Constrained IoT Environments," Proc. 5th IEEE World Forum on Internet of Things (WF-IoT), Limerick, Ireland, April 2019.
  13. V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, "Interledger Smart Contracts for Decentralized Authorization to Constrained Things," Proc. 2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2019), in conjunction with IEEE INFOCOM 2019, Paris, France, April-May 2019.
  14. N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, G.C. Polyzos, "Secure IoT access at scale using blockchains and smart contracts," Proc. 8th IEEE WoWMoM Workshop on the Internet of Things: Smart Objects and Services (IoT-SoS), Washington DC, USA, June 2019.
  15. N. Fotiou, G.C. Polyzos, "Name-based security for Information-Centric Networking architectures," *Future Internet*, vol. 11, no. 11, November 2019 (<https://doi.org/10.3390/fi11110232>).
  16. N. Fotiou, I. Pittaras, V.A. Siris, G.C. Polyzos, "Enabling opportunistic users in multi-tenant IoT systems using decentralized identifiers and permissioned blockchains," Proc. Workshop on the Internet of Things Security and Privacy (IoT S&P), in conjunction with the 26th ACM Conference on Computer and Communications Security (CCS), London, UK, November 2019 (poster).
  17. N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, G.C. Polyzos, "Poster: Securing IoT services using DLTs and Verifiable Credentials," Proc. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2020 (poster).
  18. N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, G.C. Polyzos, "OAuth 2.0 Authorization using Blockchain-based Tokens," Proc. Workshop on Decentralized IoT Systems and Security (DISS) in conjunction with the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2020.
  19. C. Karapapas, I. Pittaras, G.C. Polyzos, "Fully Decentralized Trading Games with Evolvable Characters Using NFTs and IPFS," Proc. workshop on Decentralising the Internet with IPFS and Filecoin, in conjunction with IFIP Networking, June 2021.
  20. N. Fotiou, Y. Thomas, V.A. Siris, G. Xylomenos, G.C. Polyzos, "Securing Named Data Networking Routing using Decentralized Identifiers," Proc. SARNET-21 workshop, IEEE International Conference on High Performance Switching and Routing (HPSR), Paris, France, June 2021.
  21. N. Fotiou, V.A. Siris, G.C. Polyzos, "Enabling Self-Verifiable Mutable Content Items in IPFS Using Decentralized Identifiers," Proc. workshop on Decentralising the Internet with IPFS and Filecoin, in conjunction with IFIP Networking, June 2021.

22. N. Fotiou, V.A. Siris, G.C. Polyzos, "Capability-based access control for multi-tenant systems using OAuth 2.0 and Verifiable Credentials," Proc. 30th International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, July 2021 (invited paper).
23. I. Pittaras, N. Fotiou, V.A. Siris, G.C. Polyzos, "Beacons and Blockchains in the Mobile Gaming Ecosystem: A Feasibility Analysis," Sensors, vol. 21, no. 3, January 2021.
24. N. Fotiou, I. Pittaras, V.A. Siris, G.C. Polyzos, P. Anton, "A privacy-preserving statistics marketplace using local differential privacy and blockchain: An application to smart-grid measurements sharing," Blockchain: Research and Applications, vol. 2, no. 1, April 2021.  
(<https://www.sciencedirect.com/science/article/pii/S2096720921000178>)
25. N. Fotiou, Y. Kortensniemi, D. Lagutin, V.A. Siris, G.C. Polyzos, "Capabilities-based access control for IoT devices using Verifiable Credentials," Proc. IEEE Workshop on the Internet of Safe Things, in conjunction with the 43rd IEEE Symposium on Security and Privacy, San Francisco, CA, USA, May 2022.
26. 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.
27. N. Fotiou, E. Faltaka, V. Kalos, A. Kefala, I. Pittaras, V.A. Siris, G.C. Polyzos, "Continuous authorization over HTTP using Verifiable Credentials and OAuth 2.0," Proc. Open Identity Summit, Copenhagen, DK, July 2022.