

**Allkirjad elektroonilistel dokumentidel : vääramatu tõenduse algoritmidest**

**Buldás, Ahto** A & A 2000 / 6, lk. 36-40

**A blockchain-assisted hash-based signature scheme**

**Buldás, Ahto; Laanoja, Risto; Truu, Ahto** Secure IT Systems : 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018 : proceedings 2018 / p. 138-153 : ill [https://doi.org/10.1007/978-3-030-03638-6\\_9](https://doi.org/10.1007/978-3-030-03638-6_9) [Conference Proceedings at Scopus](#) [Article at Scopus](#) [Conference Proceedings at WOS](#) [Article at WOS](#)

**BLT+L : efficient signatures from timestamping and endorsements**

**Firsov, Denis; Lakk, Henri; Laur, Sven; Truu, Ahto** Proceedings of the 18th International Conference on Security and Cryptography - SECRIPT. Vol. 1 2021 / p. 75-86 <https://doi.org/10.5220/0010530000750086>

**Cybernetica ja TalTech asuvad koostöös uurima tuleviku digiallkirju**

Mente et Manu 2021 / lk. 12 : fot [https://www.ester.ee/record=b1242496\\*est](https://www.ester.ee/record=b1242496*est)

**Cybernetica ja TalTech asuvad koostöös uurima tuleviku digiallkirju [Võrguväljaanne]**

postimees.ee 2021 ["Cybernetica ja TalTech asuvad koostöös uurima tuleviku digiallkirju"](#)

**Development of cross boarder electronic services based on digital signatures [Electronic resource]**

**Tepandi, Jaak** eBaltics : Building Effective Partnership Networks : Baltic ITAMPT 2003 : Riga, April 2-5, 2003 2003 / [CD-ROM]

**Digiallkirja isa Tarvi Martens : "Skype"ist lahkumine oli võib-olla finantsiliselt elu kõige viletsam otsus"**

Änilane, Eleen digipro.geenius.ee 2022 [Digiallkirja isa Tarvi Martens: "Skype"ist lahkumine oli võib-olla finantsiliselt elu kõige viletsam otsus"](#)

**Digital signature systems - an interoperability outlook**

**Tšahhírov, Ilja; Bolotov, Jevgeni; Tepandi, Jaak** Scientific proceedings of Riga Technical University. 5. [series], Computer science 2004 / p. 60-68

**Digital signatures in interoperable electronic services**

**Tepandi, Jaak** Baltic ITAMPT review 2003 / 3, p. 62-65 [https://artiklid.elnet.ee/record=b2025607\\*est](https://artiklid.elnet.ee/record=b2025607*est)

**Eestis arendatud plokiahel soovib saada maailmaturu liidriks**

Rumm, Hannes Eesti Ekspress 2023 / lk. 30-33 <https://dea.digar.ee/article/eestiekspress/2023/05/10/13.6>

**Efficient long-term validation of digital signatures**

Ansper, A.; **Buldás, Ahto**; Roos, Meelis; Willemson, Jan Public Key Cryptography : 4th International Workshop on Practice and Theory in Public Key Cryptosystems : PKC 2001 : Cheju Island, Korea, February 13-15, 2001 : proceedings 2001 / p. 13-15

**e-identity : a step forward to European Digital Citizenship**

**Ramiro Troitino, David; Mazur, Viktoria** E-Governance in the European Union : strategies, tools, and implementation 2024 / p. 57-70 [https://doi.org/10.1007/978-3-031-56045-3\\_5](https://doi.org/10.1007/978-3-031-56045-3_5) [https://www.ester.ee/record=b5703480\\*est](https://www.ester.ee/record=b5703480*est)

**Ekspert: eestlastel on olemas teadmised küberturvalisusest, kuid millegipärast neid ei kasutata [Võrguväljaanne]**

**Baum, Anu** geenius.ee 2022 [Ekspert: eestlastel on olemas teadmised küberturvalisusest, kuid millegipärast neid ei kasutata](#)

**Electronic signature system with small number of private keys**

**Buldás, Ahto; Saarepera, Märt** 2nd Annual PKI Research Workshop Pre-Proceedings : Gaithersburg, Maryland, USA, April 28-29, 2003 2003 / p. 96-108 [https://www.researchgate.net/publication/2869630\\_Electronic\\_Signature\\_System\\_with\\_Small\\_Number\\_of\\_Private\\_Keys](https://www.researchgate.net/publication/2869630_Electronic_Signature_System_with_Small_Number_of_Private_Keys)

**Hash-based server-assisted digital signature solutions = Räsifunktsioonidel põhinevad serveri toega digitaalse signeerimise lahendused**

**Truu, Ahto** 2020 <https://digikogu.taltech.ee/et/Item/a972cc4b-53ec-4c82-8de0-b3e941cce345>

**Inimese roll logistikas kasvab kriisi ajal jõudsalt : intervjuu**

**Janno, Jelizaveta** Äripäev 2020 / lk. 26-27 : portr [https://www.ester.ee/record=b2122331\\*est](https://www.ester.ee/record=b2122331*est)

**Interoperability of digital signatures - a priority in Northern eSecurity**

**Tepandi, Jaak; Ott, Arvo** Baltic ITAMPT review 2002 / 2, p. 42-44 [https://artiklid.elnet.ee/record=b2024788\\*est](https://artiklid.elnet.ee/record=b2024788*est)

**Keyless signature infrastructure and PKI : hash-tree signatures in pre- and post-quantum world**

**Buldás, Ahto; Laanoja, Risto; Truu, Ahto** International journal of services technology and management 2017 / p. 117-130 : ill <https://doi.org/10.1504/IJSTM.2017.10002708> [Journal metrics at Scopus](#) [Article at Scopus](#)

**Keyless signatures' infrastructure: How to build global distributed hash-trees**

**Buldas, Ahto**; Kroonmaa, Andres; **Laanoja, Risto** Secure IT Systems : 18th Nordic Conference, NordSec 2013, Ilulissat, Greenland, October 18-21, 2013, Proceedings 2013 / p. 313 - 320 [https://doi.org/10.1007/978-3-642-41488-6\\_21](https://doi.org/10.1007/978-3-642-41488-6_21) [Conference Proceedings at Scopus](#) [Article at Scopus](#)

### **Küberohud meie nina all: 4 igapäevast turvariski, mida tõsiselt ei võeta [Võrguväljaanne]**

digipro.geenius.ee 2022 [Küberohud meie nina all: 4 igapäevast turvariski, mida tõsiselt ei võeta](#)

### **Lahendus tulevikuks - PKI : ülevaade**

**Sepp, Olev** A & A 2000 / 1, lk. 35-45 [https://artiklid.elnet.ee/record=b1003332\\*est](https://artiklid.elnet.ee/record=b1003332*est)

### **Long term archiving of electronic signatures**

**Buldas, Ahto**; Freudenthal, Margus Baltic ITAMPT review 2004 / 1, p. 69-74 : ill

### **A New approach to constructing digital signature schemes**

**Buldas, Ahto; Frisov, Denis; Laanoja, Risto**; Lakk, Henri; **Truu, Ahto** Advances in Information and Computer Security : 14th International Workshop on Security, IWSEC 2019, Tokyo, Japan, August 28–30, 2019 : proceedings 2019 / p. 363-373 [https://doi.org/10.1007/978-3-030-26834-3\\_21](https://doi.org/10.1007/978-3-030-26834-3_21) [Conference proceeding at Scopus](#) [Article at Scopus](#) [Conference proceeding at WOS](#) [Article at WOS](#)

### **An overview of digital signing and the influencing factors in Estonian local governments**

Felt, Sigrid; **Pappel, Ingmar; Pappel, Ingrid** Future Data and Security Engineering : Third International Conference, FDSE 2016, Can Tho City, Vietnam, November 23-25, 2016 : proceedings 2016 / p. 371-384 : ill [https://doi.org/10.1007/978-3-319-48057-2\\_26](https://doi.org/10.1007/978-3-319-48057-2_26) [Conference Proceedings at Scopus](#) [Article at Scopus](#) [Conference Proceedings at WOS](#) [Article at WOS](#)

### **Paranoia või suure venna sünd? Digiallkirja kehtivuse kontrollimiseks läheb dokument kogu täiega riigi kätte! Miks? [Võrguväljaanne]**

Pämapuu, Priit ohtuleht.ee 2021 ["Paranoia või suure venna sünd?"](#)

### **Re-shaping the EU digital identity framework**

**Lips, Silvia**; Vinogradova, Natalia; Krimmer, Robert Johannes; **Draheim, Dirk** 23rd Annual International Conference on Digital Government Research (DGO2022) : Intelligent Technologies, Governments and Citizens, June 15-17, 2022 : proceedings 2022 / p. 13-21 <https://doi.org/10.1145/3543434.3543652> [Conference proceedings at Scopus](#) [Article at Scopus](#)

### **A server-assisted hash-based signature scheme**

**Buldas, Ahto; Laanoja, Risto; Truu, Ahto** Secure IT Systems : 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8-10, 2017 : proceedings 2017 / p. 3-17 : ill [https://doi.org/10.1007/978-3-319-70290-2\\_1](https://doi.org/10.1007/978-3-319-70290-2_1) [Conference proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

### **Systematic digital signing in Estonian e-Government processes : influencing factors, technologies, change management**

**Pappel, Ingrid**; Pappel, Ingmar; **Tepandi, Jaak; Draheim, Dirk** Transactions on large-scale data- and knowledge-centered systems XXXVI : special issue on data and security engineering 2017 / p. 31-51 : ill [https://doi.org/10.1007/978-3-662-56266-6\\_2](https://doi.org/10.1007/978-3-662-56266-6_2) [Conference proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

### **The hybrid smart contract agreement challenge to European electronic signature regulation**

Veerpalu, Anne; Jürgen, Liisi; Rodrigues E Silva, Eduardo Da Cruz; Norta, Alexander International journal of law and information technology 2020 / 45 p. <https://doi.org/10.1093/ijlit/eaab005> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

### **TOPCOAT: towards practical two-party Crystals-Dilithium**

**Snetkov, Nikita; Vakarjuk, Jelizaveta**; Laud, Peeter Discover computing 2024 / art. 18, 31 p. <https://doi.org/10.1007/s10791-024-09449-2> [Journal metrics at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

### **Verified multiple-time signature scheme from one-time signatures and timestamping**

**Firsov, Denis; Lakk, Henri; Truu, Ahto** 2021 IEEE 34th Computer Security Foundations Symposium (CSF) 2021 / 13 p <https://doi.org/10.1109/CSF51468.2021.00051>

### **Verified security of BLT signature scheme**

**Firsov, Denis; Buldas, Ahto; Truu, Ahto; Laanoja, Risto** CPP 2020 - Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, co-located with POPL 2020, New Orleans 20 January 2020 through 21 January 2020 / p. 244-257 <https://doi.org/10.1145/3372885.3373828>