Verifiability of Scytl's voting system for government elections

Scytl Election Technologies SLU
08021 Barcelona, Spain
www.scytl.com

Scytl's online voting system has been a pioneer in the introduction of verifiability in online voting schemes for political elections. Starting from 2004 in Switzerland (Neuchâtel), Scytl's voting system included voting receipts [1], allowing voters to check that their vote was present in the final tally. In Norway, in 2011 and 2013, Scytl's online voting system introduced cast-as-intended individual verifiability for the first time in a national election using return codes [2], and counted-as-recorded verifiability using universal verifiable Mix-nets [3,4]. In 2015, Scytl's voting system implemented a second verification mechanism designed for the State of New South Wales (Australia), based on a cast and decrypt approach (decryption of the vote in a trusted environment accessible by phone) [5]. This mechanism was improved in 2019 State election by using a mobile verification application. Also in 2015, Scytl's individual verifiability (return codes) was adopted in Switzerland (Neuchâtel) and achieved in 2017 the Swiss certification for individual verifiable systems [6]. Currently, Scytl's online voting system has been selected by 41 local authorities for the 2022 Ontario municipal elections in Canada.

In the demo session, Scytl will show the verifiability mechanisms present in the online voting system that will be available in these Canadian municipal elections.

1. Puiggalí, J., Morales-Rocha, V.: Independent voter verifiability for remote electronic voting. In: Proceedings of International Conference on Security and Cryptography (SECRYPT '07), pp. 333–336, Barcelona (2007).
2. Puiggalí, J., Guasch, S.: Universally verifiable efficient re-encryption mixnet. In: Electronic Voting 2010 (EVOTE 2010), 4th International Conference, LNI, vol. 167, pp. 241–254, Austria (2010).
3. Puiggalí, J., Guasch, S.: Cast-as-intended verification in Norway. In: 5th International Conference on Electronic Voting 2012, (EVOTE 2012), LNI, vol. 205, pp. 49–63, Austria (2012).
4. Wikström, D.: A sender verifiable mix-net and a new proof of a shuffle. In: Proceedings of the 11th International Conference on Theory and Application of Cryptology and Information Security. pp. 273–292. ASIACRYPT'05, Springer-Verlag, Berlin, Heidelberg (2005).
5. Brightwell, I., Cucurull, J., Galindo, D., Guasch, S. An overview of the iVote 2015 voting system. Tech. rep. New South Wales Electoral Commission (2015).
6. Scytl News - https://www.scytl.com/news/scytl-swiss-post-online-voting-solution-first-switzerland-certified-50-voters/