Glossari

E-voting Basilea-Citad / Grischun / Son Gagl / Turgovia

Auturs	**Direcziun Project E-voting (BS)** **Incumbensà per e-voting (GR)** **Direcziun Informatica ed infrastructura (SG)** **Persuna spezialisada per e-voting (TG)**

Data	28-04-2023
Versiun	1.1
Classificaziun	Nagina

Controlla da las midadas

Versiun	Data	Descripziun	Num
1.0	21-12-2022	Versiun dada liber	Direcziun Project E-voting (BS) Direcziun Informatica ed infrastructura (SG) Persuna spezialisada per e-voting (TG)
1.1	28-04-2023	Integraziun dal Grischun Cumplettaziuns ed adattaziuns en la part 2	Direcziun Project E-voting (BS) Incumbensà per e-voting (GR) Direcziun Informatica ed infrastructura (SG) Persuna spezialisada per e-voting (TG)

Posts d'examinaziun/da deliberaziun

Examinà tras	Dà liber tras	Data
Direcziun Dretg e dretgs politics (BS) Direcziun Servetsch per dretgs politics (SG) Direcziun Servetsch giuridic (TG)	Direcziun Dretg e dretgs politics (BS) Direcziun Servetsch per dretgs politics (SG) Direcziun Servetsch giuridic (TG)	12-12-2022
Direcziun Partiziun Servetschs (GR)		14-04-2023

Documents referenziads

Nr.	Document	Versiun
[1]	Ordinaziun da la ChF davart la votaziun electronica (OVE; CS 161.116) dals 25 da matg 2022	Versiun dal 01-07-2022
[2]	Mussavia da la Chanzlia federala per giuditgar las ristgas dal sistem dad e-voting da la Posta svizra («Mussavia per giuditgar las ristgas») https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Leitfaden%20BK_Risikobeurteilungen%20Vote%20%C3%A9lectronique,%20Oktober%202022.pdf.download.pdf/Leitfaden%20BK_Risikobeurteilungen%20Vote%20%C3%A9lectronique,%20Oktober%202022.pdf	Versiun dals 04-10-2022

Cuntegn

1 Intent dal document

Quest document descriva las noziuns ch'ils chantuns dovran en il rom da la votaziun electronica. Sch'i vegnan duvradas autras noziuns en ils documents da la Posta u en l'Ordinaziun da la ChF davart la votaziun electronica (guardar *document referenzià [1]*), vegn quai menziunà.

Per motivs da survesaivladad è il glossari dividì en dus secturs parzials: in sectur per las noziuns generalas da la votaziun electronica, l'auter sectur per las noziuns tecnicas.

1.1 Indicaziun da las funtaunas da las definiziuns originaras

Nua che quai è stà disponibel è raschunaivel, èn vegnidas duvradas – sco basa – las declaraziuns da las significaziuns en ils documents «Mussavia per giuditgar las ristgas» (guardar *document referenzià [2]*) ed «Ordinaziun da la ChF davart la votaziun electronica» (guardar *document referenzià [1]*). Las definiziuns originaras da las noziuns menziunadas èn mintgamai marcadas cun in segn spezial.

Segn spezial	Funtauna da la definiziun originara
*	Mussavia da la Chanzlia federala per giuditgar las ristgas
**	Ordinaziun da la ChF davart la votaziun electronica

Tabella 1: Attribuziun dals segns spezials tenor funtauna

1.2 Differenzas chantunalas

En tscherts cas sa differenzieschan las relaziuns chantunalas. Questas differenzas èn inditgadas en quest document ed en tut ils auters documents cuminaivels con colurs:

Colur	Chantun
violet	Text violet vala mo per il chantun Basilea-Citad
cotschen	Text cotschen vala mo per il chantun Grischun
verd	Text verd vala mo per il chantun Son Gagl
blau	Text blau vala mo per il chantun Turgovia

Tabella 2: Indicaziun da las differenzas chantunalas cun colurs

2 Glossari – noziuns generalas

La suandanta tabella dat ina survista da las noziuns generalas relevantas en connex cun la votaziun electronica.

Noziun	Descripziun
admin board	Persunas ch'èn responsablas per la realisaziun tecnica da la votaziun u elecziun.
program da bug bounty	In program da bug bounty è in «program da premias» che ha l'intent da scuvrir e d'annunziar puncts debels. Programs da bug bounty dattan impuls per la verificaziun publica (en spezial tras uschenumnads hackers etics) e contribueschan a la segirezza dad e-voting, tras quai che puncts debels pon vegnir chattads ed eliminads a temp. La Posta ha publitgà il code da funtauna sco er la documentaziun davart il sistem ed il manaschi a partir da l'onn 2021 sin la plattaforma spezialisada GitLab. En il rom da ses program da bug bounty paja ella fin 250 000 francs per annunzias che gidan a meglierar il sistem.
votaziun per correspundenza, votaziun a l'urna*	Totalitad dals cedels da votar e dals cedels electorals ch'èn vegnids dads giu per correspundenza u a l'urna.
container	Noziun da la metodologia «OCTAVE Allegro»: meds (fisics u tecnics) ch'elavuran, arcunan u transmettan resursas d'infurmaziuns.
D0*	Unitad da temp entaifer il process: Preparaziun da la votaziun u elecziun.
D1*	Unitad da temp entaifer il process: Il di, che las urnas electronicas vegnan configuradas e transmessas al sistem online da la Posta e ch'ils attests da votar vegnan generads.
D2*	Unitad da temp entaifer il process: Il di, che las clavs da segirezza per la votaziun u elecziun vegnan fixadas (cf. noziun «clav da segirezza»), che la configuraziun da la votaziun u elecziun vegn verifitgada e che las urnas electronicas vegnan preparadas.
D3*	Unitad da temp entaifer il process: Il di, che las vuschs electronicas vegnan decodadas, ch'ils resultats da la votaziun electronica vegnan eruids e che la votaziun u elecziun vegn examinada tras las examinaturas ed ils examinaturs.

Noziun	Descripziun
D4*	Unitad da temp entaifer il process: Elavuraziun posteriura da la votaziun u elecziun, incl. destrucziun da las datas.
electoral board (OVE: examinaturas ed examinaturs)	Persunas ch'èn responsablas tenor il dretg chantunal per survegliar il decurs regular da la votaziun u elecziun electronica e che surpiglian la rolla da las examinaturas e dals examinaturs tenor la OVE. Ellas genereschan la clav da segirezza per la votaziun u elecziun (cf. noziun «clav da segirezza»). En il chantun Basilea-Citad agescha il Comité electoral sco electoral board (Verordnung über den Testbetrieb für die elektronische Stimmabgabe, art. 8a). En il chantun Grischun agescha la Cumissiun per elecziuns e votaziuns cun e-voting sco electoral board (Ordinaziun davart ils dretgs politics en il chantun Grischun, art. 21g). En il chantun Son Gagl agescha in comité dal Biro da votaziun chantunal sco electoral board (WAG, art. 11 ss.). En il chantun Turgovia agescha il Biro da votaziun per Svizras e Svizzers a l'exteriur sco electoral board (StWV, art. 26).
register electoral VE*	Register chantunal da las persunas cun dretg da votar ch'èn admessas a la votaziun electronica.
resultats VE*	Resultats da la dumbraziun da las urnas electronicas.
object da la votaziun u elecziun*	Dumondas da votaziun che vegnan suttamessas a las persunas cun dretg da votar en cas votaziuns resp. glistas da candidatas e candidats en cas d'elecziuns.
meds auxiliars per las persunas cun dretg da votar	Documents e cuntegns che vegnan mess a disposiziun per infurmar las persunas cun dretg da votar (p.ex. material da votar, plattafurma d'infurmaziun e.u.v.).
resursas d'infurmaziun*	Noziun da la metodologia «OCTAVE Allegro»: Elements da datas spezialmain impurtantas. Lur integritad, confidenzialitad e/u disponibladad sto vegnir protegida.
urna da controlla	Urna che cuntegna las vuschs da controlla da las commembras e dals commembers da l'electoral board, per laschar controllar l'integritad da l'urna tras l'electoral board.
attest da votar (AdV)*	In document che permetta a las persunas cun dretg da votar, da far diever da lur dretg da votar.

Noziun	Descripziun
urnas da test	Urnas che permettan da testar la funcziunalitad dal sistem. Durant il process vegnan activadas differentas urnas da test, p.ex. vegnan dadas giu e decodadas – il di D2 – vuschs da test en preschientscha da l'electoral board, per garantir che l'entir process funcziunia correctamain.

Tabella 3: Noziuns generalas

3 Glossari – noziuns tecnicas

La suandanta tabella dat ina survista da las noziuns tecnicas relevantas en connex cun la votaziun electronica.

Noziun	Descripziun
backend*	Il backend dals conturns dad e-voting vegn manà da la Posta. El cumpiglia il server dad e-voting sco er las cumponentas da controlla.
computer chantunal	Plaz da lavur da biro normal d'ina collavuratura u d'in collavuratur dal chantun.
computer da configuraziun (offline) (OVE: cumponenta da setup) (Posta: Setup SDM)	Apparat offline, che vegn duvrà per configurar ina votaziun u elecziun (cf. noziun «apparats offline»). Sin quest apparat vegnan p.ex. generads ils codes per ils attests da votar. En spezial vegn installada la software SDM sin quest apparat.
purtaders da datas	Sticks USB u cartas SD, che vegnan duvradas per barattar datas tranter ils differents apparats.
computer da decodaziun (offline) (OVE: cumponenta da controlla tar il chantun) (Posta: Tally SDM)	Apparat offline, che vegn duvrà per maschadar e per decodar las vuschs (cf. noziun «apparats offline»). En spezial vegn installada la software SDM sin quest apparat.
DIS (data integration service)*	Tool da la Posta per generar las datotecas da configuraziun d'ina votaziun u elecziun.
entropia	En la criptografia signifitga entropia l'imprevisibilitad da datas. Pli gronda che l'entropia è, e pli cumplexas ed imprevisiblas che las datas èn. Uschia daventi pli difficil da decodar las datas. Per la segirezza dad e-voting èsi necessari che valurs, che ston esser casualas, èn casualas avunda ed han perquai in'entropia suffizienta.
sistem per l'eruida dals resultats	Sistem chantunal per dumbrar e per consolidar ils resultats da tut ils chanals da votaziun.
landing page dad e-voting	Pagina d'internet che la Posta metta a disposiziun als chantuns. La landing page cuntegna differentas infurmaziuns per las persunas cun dretg da votar sco er links a las votaziuns ed elecziuns activas sin il portal d'elecziuns e votaziuns.

Noziun	Descripziun
server dad e-voting (OVE: part dal sistem betg fidabla) (Posta: server da votaziun)	Cumponenta centrala da la plattafurma dad e-voting, sin la quala il chantun installescha la votaziun u elecziun sur il SDM. Il server dad e-voting è ina part dal backend (cf. noziun «backend»). El vegn manà da la Posta ed arcuna las urnas electronicas.
valur da hash («impronta dal det»)	Ina valur da hash (er numnada summa da controlla) è ina valur che vegn generada or da datas tras ina funcziun criptografica. Ella è ina spezia dad «impronta dal det» da las datas. Ella sa cumpona d'in dumber fix da bytes e serva ad identifitgar cler e bain las datas. Valurs da hash vegnan applitgadas per garantir l'integritad da datas. Tras mintga midada da las datas resulta ina valur da hash dal tuttafatg differenta. Sche la valur da hash è identica, san ins, ch'i n'èn vegnidas fatgas naginas midadas. Valurs da hash èn p.ex. impurtantas per producir la software necessaria per e-voting (build). A maun da las valurs da hash pon ils chantuns controllar, ch'els exequeschian la dretga software e che la software na saja betg vegnida midada (cf. noziun «trusted build e trusted deployment»).
code d'inizialisaziun sin l'attest da votar	Il code d'inizialisaziun consista d'ina retscha da cifras e da bustabs che sa chattan sin l'attest da votar. Sin la pagina d'entrada dal portal d'elecziuns e votaziuns ston las persunas cun dretg da votar endatar il code d'inizialisaziun sco er in'ulteriura caracteristica d'autentificaziun, quai per s'identifitgar e per cumenzar cun il process da votaziun.
KeePass	Manager da pleds-clav che vegn duvrà per in'administraziun segira dals pleds-clav.
cumponentas da controlla**	Las cumponentas da controlla èn elements dal sistem independents. Ellas èn concepidas differentamain, vegnan manadas da differentas persunas ed èn segiradas tras mesiras spezialas. Tschertas cumponentas da controlla èn ina part dal backend (cf. noziun «backend»), vegnan manadas da la Posta e vegnan applitgadas en spezial per generar ils codes da controlla, per controllar ils codes da controlla a chaschun da la votaziun e per maschadar las urnas. Per maschadar las urnas funghescha il computer da decodaziun sco cumponenta da controlla che vegn manada tar il chantun.
logs*	Datas che permettan da constatar ch'il process da votar funcziunia correctamain, u d'examinar in'eventuala faussa funcziun.

Noziun	Descripziun
apparats offline	Apparats isolads che vegnan duvrads per realisar e per verifitgar ina votaziun u elecziun. Ils apparats offline n'han mai access ad ina rait u a l'internet. Las datas vegnan transmessas unicamain en furma codada sur purtaders da datas (cf. noziuns «computer da configuraziun» e «computer da decodaziun»).
parameters da la votaziun u elecziun*	Datas da basa da la votaziun u elecziun, p.ex. la data da la votaziun u elecziun, las datas e las uras, durant las qualas igl è pussaivel da vuschar, il gener da la votaziun e/u elecziun sco er ils parameters da segirezza (p.ex. il dumber da commembras e commembers da l'electoral board).
pleds-clav da la votaziun u elecziun	Pleds-clav per generar la clav da segirezza da la votaziun u elecziun il di D2 (las clavs da segirezza vegnan duvradas per codar e per decodar las vuschs).
pleds-clav da las commembras e dals commembers da l'admin board	Pleds-clav che permettan ad ina commembra u ad in commember da l'admin board da s'autentifitgar tar il SDM (cf. noziun «SDM (Secure Data Manager)»).
SDM (Secure Data Manager)*	Software centrala da la Posta, che permetta als chantuns da preparar e da realisar ina votaziun u elecziun. Questa software vegn installada sin ils computers dad e-voting dals chantuns. Cun questa software vegnan p.ex. generads ils codes per las persunas cun dretg da votar e las clavs da segirezza per codar las vuschs (dis D1 e D2) sco er maschadadas e decodadas las vuschs (di D3).
seed	Seed (englais per semenza, semnar) designescha en la criptografia la valur iniziala (valur d'inizialisaziun) per in algoritmus da codaziun. Sin basa dal seed che vegn endatà dal chantun, vegnan calculads ils parameters da codaziun.
clav da segirezza	Crap da fundament criptografic per proteger in asset digital. En il context da la votaziun electronica vegn generada – sin basa da l'endataziun da dus pleds-clav – la clav da segirezza per codar e per decodar las vuschs.
software dals servetschs d'abitants	Applicaziun (software) da las vischnancas u dals chantuns per administrar e per tgirar las datas da las persunas cun dretg da votar. L'applicaziun vegn plinavant duvrada per generar las datotecas eCH0045 (register electoral) per la votaziun u elecziun (cf. noziun «register electoral VE»).
software per generar ils attests da votar*	Software che vegn duvrada per generar ils attests da votar.

Noziun	Descripziun
computer per ils attests da votar (AdV) (offline)	Apparat offline, che vegn duvrà per generar ils attests da votar.
computer da sincronisaziun (online) (OVE: part dal sistem betg fidabla) (Posta: Online SDM)	Apparat online, che vegn duvrà per sincronisar la votaziun u elecziun cun ils servers da la Posta. En spezial vegn installada la software SDM sin quest apparat.
trusted build e trusted deployment	La noziun trusted build e trusted deployment (curt «trusted build e deployment») stat per la producziun fidabla (build) e per l'installaziun fidabla (deployment) da la software che vegn duvrada per e-voting. Tras il process da trusted build e trusted deployment vegni garantì, che la software utilisada da la Posta e dals chantuns correspundia al code da funtauna publitgà. Il code da funtauna vegn suttamess ordavant ad ina controlla publica ed ad ina verificaziun independenta. Quest process vegn accumpagnà activamain tras ina persuna spezialisada incaricada dals chantuns, sco er tras ina represchentanta u in represchentant dals chantuns. Ils protocols respectivs vegnan publitgads.
computer da verificaziun (offline)	Apparat offline, che vegn mess a disposiziun a l'electoral board per verifitgar la votaziun u elecziun (cf. noziun «apparats offline»). En spezial vegn installada la software Verifier sin quest apparat.
Verifier* (OVE: med auxiliar tecnic da las examinaturas e dals examinaturs)	Software da la Posta. Il Verifier serva a las examinaturas ed als examinaturs sco med auxiliar tecnic per verifitgar la configuraziun da la votaziun u elecziun sco er la maschaida e la decodaziun.
codes da verificaziun sin l'attest da votar*	Ils codes stampads sin l'attest da votar (code da conferma, code da finalisaziun sco er codes da controlla).
portal d'elecziuns e votaziuns*	Portal d'internet da la Posta, che vegn duvrà da las persunas cun dretg da votar per vuschar.

Tabella 4: Noziuns tecnicas

4 Glista da las tabellas