

# Hierodiction Software

## EVOTE LGG: Logging- und Auditsystem

## EVOTE IDC: Intrusion Detection Cockpit

### “Logging” vs. Audit System

Konventionelle e-Voting-Systeme oder andere Sicherheitssoftware bietet klassisches Logging, sei es in eine Datei oder in eine (manchmal verschlüsselte) Datenbanktabelle. Dies aber bietet nicht die raschen, real-time Such- und Auditierfunktionalitäten, wie sie in einem e-Voting-System benötigt werden.

EVOTE LGG bietet ein umfassendes Auditsystem, das wie ein Data Warehouse multidimensional strukturiert ist und schnelle, punktgenaue Informationen in einer Auditsituation bietet.

### Vorteile

**Customisierbarkeit:** LGG kann leicht an Ihre Auditerfordernisse angepasst werden, indem es eine große Zahl möglicher Protokollierungspunkte bietet, die aktiviert werden können. Sehr sensible Protokollpunkte sind allerdings immer aktiv.

“alle Einträge für einen Wahlkreis”, “alle Einträge für einen Wähler”, “alle Systemalarme”.

**Vollständige Nachvollziehbarkeit:** EVOTE bietet eine große Zahl von Standardreports über den gesamte Lebenszyklus einer Wahl an. Aufgrund der Flexibilität des Produktes können kundenspezifische Reports definiert werden. Alle Komponenten inkl. VRL und SKM benutzen LGG, wodurch ein umfassender und nahtloser „Audit Trail“ sichergestellt ist.

Protokollierung	Nachricht	Status	Verpflichtung
Admin Access Change User Password procedure	Der Benutzername wurde geändert.	True	False
Vote Data Screen Save BIRTH collection	Die Wahl Protokollierung wurde gespeichert.	True	False
Save user check from user reference screen, not saved in database	Die Benutzerdaten wurden nicht.	True	False
Save voting user in database	Die aktuelle Benutzer wurde gespeichert.	True	False
Save new user in database	Der neue Benutzer wurde gespeichert.	True	False
Election access records (ACCESS) is saved	Ein Ereignisprotokoll für eine Wahl wurde modifiziert/hinzugefügt.	True	False
Registration screen save election results according the EVOTE ID	Die Wahl Protokollierung wurde gespeichert.	True	False
Log Change of change password procedure because of user name	Die Protokollierung wurde geändert.	True	False
Local event of connectivity from monitoring user who started vote	Connectivity-Loggen wurde für Benutzer.	True	False
Log in Voting User of public key login used for authentication	Log-In-Meldung wurde für Benutzer protokolliert.	True	False
Event log screen for public key login used for authentication	Connectivity-Loggen wurde für Benutzer.	True	False
Logging screen, save LOG parameters	Die Protokollierungsparameter wurden gespeichert.	True	False
General mailbox pattern detected in input string by HCheck -ill	Die Wahl Protokollierung wurde gespeichert.	True	False
Save existing election	Die Wahl Protokollierung wurde gespeichert.	True	False
In election and confidentiality load, when value cannot be verified	Verifikation des Hashwertes aus der Datenbank schlägt fehl, der Inhalt d. Wahl Protokollierung wurde gespeichert.	True	False
Save operation confidentiality monitoring	Die Wahl Protokollierung wurde gespeichert.	True	False
Mail server connection to the internet	Die Wahl Protokollierung wurde gespeichert.	True	False
Active function in ReleaseFunction was cancelled	Die Wahl wurde geschlossen und archiviert.	True	False
Release function in ReleaseFunction was reported.	Die Releasefunktion wurde durchgeführt und Fehler wurden gefunden.	True	False
Release function in ReleaseFunction was cancelled out.	Die Wahl wurde freigegeben.	True	False
Abort by user in StatusConfirmitancy	Schließen und Archivierung des Wahlbereichs von Benutzer abgebrochen.	True	False
Confirmitancy closed in StatusConfirmitancy	Die Wahl Protokollierung wurde geschlossen und archiviert.	True	False
Release function in ReleaseConfirmitancy was reported.	Die Releaseprüfung wurde durchgeführt und Fehler wurden gefunden.	True	False
Release function in ReleaseConfirmitancy was cancelled out.	Die Wahl Protokollierung wurde erfolgreich freigegeben.	True	False
Release of election in confidentiality aborted by user	Die Freigabeprüfung wurde vom Benutzer abgebrochen.	True	False
Request key communication failure with SKM	Abmeldung eines Schlüssel beim SKM scheiterte in der Freigabe einer.	True	False

**Integration in das Zugriffskonzept:** LGG ist nahtlos in das rollenbasierte Zugriffskonzept der jew. Applikation eingebunden und stellt daher sicher, dass nur die Daten eingesehen werden können, für die eine Berechtigung besteht.

**Verschlüsselung und Datenintegrität:** Selbstverständlich sind alle Protokolleinträge verschlüsselt, zusätzlich wird die Integrität aller Einträge durch Hashwerte (SHA-1) gesichert.

**Wiederverwendung:** LGG ist eine .dll unter .net mit wohldefinierten Schnittstellen und Standardreports, die von anderen Applikationen aufgerufen werden können. Da LGG mit seinem eigenen Tablespace arbeitet, kann es leicht von EVOTE separat in andere Applikationen integriert werden und da einige der Dimensionen im LGG Data Warehouse frei definierbar sind, kann LGG auch leicht an eine breite Palette von Einsatzgebieten angepasst werden.

**Multi-dimensionale Struktur:** Die Protokolleinträge werden in einer multidimensionalen Data Warehouse Struktur gespeichert, die rasche und zielgerichtete Suche ermöglicht, z.B.:

Lo.	P.	P.	Prot.	Benutzer	Zeitstempel	Sitzungs-ID	Protokolltext
66	C	0	0	Administrator	10/17/2007 1		The mail table (main data table) for the election has been created. Election: 5 Musterwahl
67	C	0	0	aprosser			An election access record has been saved/modified. Added user: aprosser
68	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
69	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
70	C	0	0	aprosser			Die Releaseüberprüfung wurde durchgeführt und Fehler wurden gefunden. Die Fr...
71	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
72	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
73	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
74	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
75	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
76	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
77	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
78	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
79	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
80	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
81	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
82	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
83	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
84	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
85	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
86	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
87	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
88	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
89	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
90	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
91	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
92	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
93	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
94	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
95	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
96	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
97	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
98	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
99	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
100	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
101	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
102	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
103	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
104	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
105	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
106	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
107	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
108	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
109	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
110	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
111	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
112	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
113	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
114	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
115	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
116	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
117	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
118	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
119	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
120	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
121	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
122	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
123	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
124	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
125	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
126	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
127	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
128	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
129	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
130	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
131	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
132	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
133	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
134	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
135	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
136	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
137	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
138	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
139	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
140	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
141	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
142	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
143	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
144	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
145	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
146	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
147	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
148	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
149	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
150	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
151	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
152	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
153	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
154	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
155	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
156	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
157	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
158	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
159	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
160	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
161	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
162	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
163	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
164	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
165	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
166	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
167	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
168	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
169	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
170	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
171	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
172	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
173	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
174	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
175	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
176	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
177	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
178	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
179	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
180	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
181	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
182	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
183	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
184	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
185	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
186	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
187	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
188	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
189	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
190	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
191	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
192	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
193	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
194	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
195	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
196	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
197	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
198	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
199	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl
200	C	0	0	aprosser			Die Wahl Protokollierung wurde gespeichert. Election: 5 Musterwahl

## Intrusion Detection Cockpit (IDC)

Das Cockpit ermöglicht es Administratoren EVOTE laufend zu überwachen, v.a. während einer Wahl. Alle Wahlsitzungen werden in LGG vermerkt und jede Anfrage eines Wahlclient wird geprüft:

- ☞ Konsistenz im Prozess,
- ☞ Timeouts,
- ☞ Schadcode

sowie eine große Zahl weiterer verdächtiger Aktivitäten. Auch die Integrität der Daten in EVOTE wird laufend geprüft.

Das Intrusion Detection Cockpit soll Systemadministratoren bei der Betriebsüberwachung unterstützen und jede verdächtige Aktivität erzeugt sofort einen Alarm in der IDC. Auch nicht böswillig herbeigeführte Fehlerzustände im System werden auf diese Weise sofort gemeldet und lenken die Aufmerksamkeit der Systemadministratoren sofort auf den Fehlerzustand. Dabei wird nach folgenden Prinzipien vorgegangen:

- ☞ laufende Überwachung aller Komponenten,
- ☞ prozessorientierte Überwachung,

- ☞ automatische Bedrohungsklassifikation,
- ☞ Zusatzinformationen zu jedem Alert,
- ☞ sofortige Benachrichtigung der Administration.

Systemaktivitäten werden nicht nur isoliert als solche überwacht, sondern im Prozesszusammenhang gesehen, wobei auch frühere Kommunikationen mit einem Partner berücksichtigt werden. Damit können **auch komplexe Bedrohungsbilder erkannt** werden.

Mit seiner weitgehend **automatisierten Überwachung und Bedrohungsklassifikation** unterstützt die IDC die Systemadministration, die ein „High-Level“ Bild der Systemaktivitäten erhält.

Gleichzeitig jedoch kann zu jedem Alert Detailinformation über Art und Quelle der möglichen Bedrohung angefordert werden, die eine effektive Antwort ermöglichen.

Die IDC deckt alle Komponenten von EVOTE ab und ergänzt so eine infrastrukturelle Intrusion Detection.

Microsoft, Windows, SQL Server und .net sind Marken der Microsoft Corporation. Java ist eine Marke von Sun Microsystems. RSA ist eine Marke der RSA Security Inc. Hierodiction ist eine Marke der Hierodiction Software GmbH.

