Politica di Crittografia del Sistema di Gestione Integrato (SGI)

Redatto da: _____ Data 10/06/2024
(firma)
Anna Veltri, DPO
(nome, cognome, qualifica)

Verificato da: _____ Data 12/06/2024
(firma)
Massimo Ortensi, Settore Sistemi
(nome, cognome, qualifica)

Approvato da: Comitato Sicurezza Data 17/06/2024
(nome, cognome, qualifica)

Versione : 2.4

Distribuzione : Distribuibile

Classificazione di sicurezza : Normale

Il documento è da ritenersi "IN LAVORAZIONE" se provvisto della sola firma: *Redatto da*
Il documento è da ritenersi "VERIFICATO ED EMESSO IN BOZZA" se provvisto anche della firma: *Verificato da*
Il documento è da ritenersi "DISTRIBUIBILE" se provvisto anche della firma: *Approvato da*

Indice

0 Storia Dei Cambiamenti

DATA	Versione	MOTIVO DEL CAMBIAMENTO
20/02/2020	1.0	Prima stesura
11/11/2021	2	Aggiornamento ragione sociale e normativa di riferimento
30/11/2022	2.1	Aggiornamento e inserimento altri servizi
07/09/2023	2.2	Aggiornamento e inserimento altri servizi
19/02/2024	2.3	Aggiornamento ragione sociale
17/06/2024	2.4	Aggiornamento logo

1 Scopo del documento

Il presente documento descrive i controlli crittografici utilizzati da Unimatica S.p.A. in conformità a leggi, regolamenti, accordi rilevanti. Nel caso di normativa specifica o nel caso di trattamento di dati personali "particolari" o di dati personali relativi "alle condanne penali e ai reati o a connesse misure di sicurezza" da parte di Unimatica, si applicano le misure di crittografia specifiche a seconda degli strumenti e delle aree aziendali coinvolti.

Il presente documento permette ai Clienti di Unimatica S.p.A. di verificare che l'uso della crittografia sia allineato con i propri requisiti.

2 Lista di distribuzione

Portale aziendale.

3 Riferimenti

Il seguente documento è redatto in conformità ai requisiti della norma ISO 9001:2015 e della norma ISO/IEC 27001:2013, comprese le estensioni di certificazione ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 27701:2019.

4 Politiche di crittografia

Unimatica S.p.A. adotta tutte le misure di crittografia definite dalla normativa specifica in relazione agli strumenti e alle aree aziendali coinvolti. Un esempio di normativa che richiede l'uso della cifratura è il GDPR, il quale infatti impone che tra le misure tecniche che il Titolare del trattamento deve mettere in atto per garantire la sicurezza dei dati personali trattati si indica la cifratura dei dati personali. Unimatica, nella sua duplice qualità di Titolare o Responsabile del trattamento, garantisce l'applicazione della tecnica di cifratura ai sensi dell'art. 32 del GDPR per il trattamento dei dati "particolari", ma in generale per tutti i dati personali trattati.

In specifico, per tutti i servizi, Unimatica garantisce la crittografia nella trasmissione dei dati su reti pubbliche attraverso l'uso del protocollo HTTPS per la comunicazione sicura (cifratura HTTPS "in-transit") e si applica la cifratura sui dischi "at-rest" predefinita.

Unimatica S.p.A. adotta le seguenti politiche di crittografia per singolo servizio

Servizio di Conservazione a norma	Si rinvia a quanto indicato nel Manuale del Servizio di conservazione a disposizione del cliente su richiesta.
Servizio di Firma	Unimatica S.p.A. non prevede di default la crittografia dei documenti sottoposti a firma (FEA OTP o FEA Grafometrica), ma prevede l'uso di canali di comunicazione tra server e client cifrati. Si applica la cifratura HTTPS "in-transit" e la cifratura sui dischi "at-rest"

	L'uso di tecniche di cifratura ulteriori possono essere concordate e adottate con il Cliente nel contratto. In relazione alle chiavi di cifratura dei vettori biometrici, si precisa che le chiavi private sono custodite in modo sicuro da uno studio notarile nostro fornitore o, in generale, dal fornitore della chiave stessa se qualche Cliente richiede di generarla da altro fornitore; la chiave pubblica è salvata sul DB per l'uso applicativo.
Servizio di Siope+	Il servizio non prevede l'utilizzo di crittografia per i documenti oggetto dello stesso; opera attraverso canali di comunicazione cifrati ed autenticati. Si applica la cifratura HTTPS "in-transit" e la cifratura sui dischi "at-rest". L'utilizzo di tecniche di cifratura addizionali può essere messo a disposizione del cliente, qualora concordate e/o oggetto di requisito contrattuale.
Servizio di Fatturazione elettronica	Il servizio non prevede la crittografia dei documenti in oggetto; opera attraverso canali di comunicazione cifrati ed autenticati ed in particolare viene crittografata la comunicazione con il SDI, così come richiesto dalle relative specifiche. Si applica la cifratura HTTPS "in-transit" e la cifratura sui dischi "at-rest" Ulteriori tecniche di crittografia possono essere concordate con il cliente all'interno del contratto.
Servizio di Gestione documentale	Il servizio non prevede l'utilizzo di crittografia per i documenti oggetto dello stesso; opera attraverso canali di comunicazione cifrati ed autenticati. Si applica la cifratura HTTPS "in-transit" e la cifratura sui dischi "at-rest". L'utilizzo di tecniche di cifratura addizionali può essere messo a disposizione del cliente, qualora concordate e/o oggetto di requisito contrattuale.
Servizio di Archiviazione in cloud	Il servizio esegue la cifratura automatica di tutti i documenti presi in carico con algoritmo AES-CBC con chiave a 128 bit; i documenti vengono quindi archiviati in forma cifrata e decifrati solo al momento del loro download richiesto da utente autorizzato. Si applica la cifratura HTTPS "in-transit" e la cifraturasui dischi "at-rest"
Servizio di videocollaborazione	Il servizio non prevede l'utilizzo di crittografia per i documenti oggetto dello stesso, opera attraverso canali di comunicazione cifrati ed autenticati. Si applica la cifratura HTTPS "in-transit" e la cifratura sui dischi "at-rest". L'utilizzo di tecniche di cifratura addizionali può essere messo a disposizione del cliente, qualora concordate e/o oggetto di requisito contrattuale.
Servizio di notifiche	Il servizio non prevede l'utilizzo di crittografia per i documenti oggetto dello stesso; opera attraverso canali di comunicazione cifrati ed autenticati. Si applica la cifratura HTTPS "in-transit" e la cifratura sui dischi "at-rest". L'utilizzo di tecniche di cifratura addizionali può essere messo a disposizione del cliente, qualora concordate e/o oggetto di requisito contrattuale.
Servizio di gestione pagamenti e incassi	Il servizio non prevede l'utilizzo di crittografia per i documenti oggetto dello stesso; opera attraverso canali di comunicazione cifrati ed autenticati. Si applica la cifratura HTTPS "in-transit" e la cifratura sui dischi "at-rest". L'utilizzo di tecniche di cifratura addizionali può essere messo a disposizione del cliente, qualora concordate e/o oggetto di requisito contrattuale.
Servizi per il cittadino	Il servizio non prevede l'utilizzo di crittografia per i documenti oggetto dello stesso; opera attraverso canali di comunicazione cifrati ed autenticati. Si applica la cifratura HTTPS "in-transit" e la cifratura sui dischi "at-rest". L'utilizzo di tecniche di cifratura addizionali può essere messo a disposizione del cliente, qualora concordate e/o oggetto di requisito contrattuale.