Appunti di Computer Security

Giuseppe Criscione

Contents

1 Kerberos

1.1 Protocollo di Needham-Schröder

1. $A \longrightarrow TTP \ : \ A, B, N_a$
2. $TTP \longrightarrow A \ : \ \{N_a, B, K_{ab}, \{K_{ab}, A\}K_b\}_{K_a}$
3. $A \longrightarrow B \ : \ \{K_{ab}, A\}_{K_b}$
4. $B \longrightarrow A \ : \ \{N_b\}_{K_{ab}}$
5. $A \longrightarrow B \ : \ \{N_b - 1\}_{K_{ab}}$

Il protocollo di Needham-Schröder vuole distribuire una chiave crittografica ai partecipanti detta anche *chiave di sessione*. La chiave è generata dal server fidato, che la impacchetta sia dentro il ticket sia dentro il messaggio (passo

2). La correttezza deriva dall'affidabilità del server mentre la segretezza del protocollo deriva dalla cifratura.

I primi tre messaggi completano lo scambio della chiave, i messaggi 4 e 5 servono a realizzare *mutua autenticazione*.

Il limite del protocollo è che i messaggi 4 e 5 sono separati dalla prima fase. Il ticket difatti è agli occhi di B del tutto nuovo, quindi B non può fare nessun tipo di controllo.

1.2 Attacco di replica

Definizione: *Spacciare informazione (chiavi, ...) obsoleta , magari violata, come recente.*

Supponiamo che C abbia violato una vecchia chiave di sessione K_{ab} che B condivise con A.

...

3. $C \longrightarrow B \ : \ \{\mathbf{K_{ab}}, \mathbf{A}\}_{\mathbf{K_b}}$
4. $B \longrightarrow A \ : \ \{N'_b\}_{K_{ab}}$
5. $C \longrightarrow B \ : \ \{N'_b - 1\}_{K_{ab}}$

B autenticherebbe A e quindi accetterebbe di usare K_{ab}.

Questo attacco prevede un potenziamento del modello di attaccante perché l'attacco funzionava se l'attaccante avesse potuto trovare una chiave di sessione vecchia. Definiamo questo attaccante DW+.

Vogliamo quindi un protocollo sicuro che risolva i limiti del precedente e vorremmo poterlo usare per accedere in maniera sicura ai servizi della nostra LAN. Ogni accesso ad un servizio di rete quindi causerebbe una procedura di autenticazione. La soluzione è Single Sing-On tramite **Kerberos**.

1.3 Accesso singolo (Single Sing-ON

Definizione: *Usare unica credenziale di autenticazione per accedere a tutti i servizi*

È una soluzione comoda ma poco robusta poiché equivale ad avere una sola password per tutto. Kerberos è un protocollo reale che si occupa di questo problema. Ciascuna delle operazioni atomiche è potenzialmente attaccabile. L'accesso singolo è potenzialmente rischioso.

1.4 Il protocollo Kerberos

Kerberos è un protocollo della fine degli anni '80 che ha come obiettivo segretezza, autentica (ad accesso singolo), temporalità. Le chiavi usate hanno validità limitata onde prevenire replay attack. Usa i timestamp, che richiedono macchine sincronizzate, contro replay attack. Il protocollo prevede tre fasi:

1. **autenticazione** con il server
2. **autorizzazione** al servizio
3. **fruizione del sevizio**

Le ultime due sono opzionali e trasparenti all'utente. Ognuna fornisce credenziali per la fase successiva:

- Fase 1 fornisce **authKey** e **authTicket** per la fase 2
- Fase 2 fornisce **servKey** e **servTicket** per la fase 3

Ogni tipo di chiave di sessione ha sua durata e una authKey può criptare diverse servKey.

1.4.1 Eventi

AS (Authentication Server) e TGS (Ticket Granting Service)

Autenticazione

1. $A \longrightarrow AS \ : \ A, TGS, T1$
2. $AS \longrightarrow A \ : \ \{authK, TGS, T_a, \{A, TGS, authK, T_a\}_{K_{tgs}}\}_{K_a}$

Autorizzazione

3. $A \longrightarrow TGS \ : \ \{A, TGS, authK, T_a\}_{k_{tgs}}, \{A, T2\}_{authK}, B$
4. $TGS \longrightarrow A \ : \ \{servK, B, T_s, \{A, BservK, T_s\}_{K_b}\}_{authK}$

Servizio

5. $A \longrightarrow B \ : \ \{A, B, servK, T_s\}_{K_b}, \{A, T_3\}_{servK}$
6. $B \longrightarrow A \ : \ \{T_3 + 1\}_{servK}$

1.4.2 Gestione delle chiavi

- AS genera authK al tempo T_a
- TGS genera servK al tempo T_s

Validità:

- authK (ossia T_a) in ore (diciamo L_a)
- servK (ossia T_s) in minuti (diciamo L_s)
- di un autenticatore (ossia T_1, T_2 e T_3) in secondi

TGS può generare servK solo qualora sia $T_s + L_s \leq T_a + L_a$ altrimenti problema di **cascata dell'attacco**.

1.4.3 Vulnerabilità

Nel timestamp risiede una vulnerabilità. $T1$, $T2$, e $T3$ li costruisce A, che non sappiamo se è onesta, quindi è presente una debolezza inerente. La falsificabilità di quel timestamp è limitata dagli istanti di creazione delle chiavi di sessione. A che serve $T1$? T1 è inerentemente debole (by design), l'unica conseguenza di questo attacco è la negazione del servizio.

Nella fase 1 A si presenta ad AS al tempo T1. Se l'attaccante blocca il messaggio allora blocca il protocollo, altrimenti AS costruisce il messaggio 2 inventando una chiave di sessione authK. Siccome As è affidabile, As impacchetta la chiave con il timestamp di creazione della stessa (Ta). Le info salienti sono impaccchettate all'interno di un pacchetto cifrato con la chiave di TGS. Alla recezione del messaggio 2, A controlla la validità temporale del messaggio. Nel messaggio 3, A inoltra il messaggio al TGS aggiungendo un autenticatore perché potrebbe non fidarsi di A. L'autenticatore è costruito con la chiave authK. Il ricevente del messaggio 3 ha evidenza di quando authK è stata creata? Si. Trova un autenticatore che decifra con successo per mezzo di questa chiave e si fida che questa chiave sia stata creata da un server che conosceva la sua chiave a lungo termine. Quindi quel timestamp lì non debba essere anteriore all'istante di creazione della chiave. Supponiamo che T2 sia minore di T3. TGS, decifrando il ticket, trova un autenticatore con un Timestamp più vecchio: abort. Il problema è che A possa volere imbrogliare l'interlocutore per convincerlo ad accettare qualcosa di più vecchio. L'autenticatore 1 è debole. La stessa cosa varrebbe per il messaggio 5 e per il messaggio 1. Questa garanzia, che è l'unica garanzia di sicurezza temporale, è il controllo sul timestamp Ts e Ta. Quindi se Ta è recente abbastanza (dato un lifetime) io accetto. Se Tb è recente abbastanza io accetto. Un'argomentazione simile vale per AS alla recezione del messaggio 1. Crypt3 trasforma un pw in una chiave. l'idea è che l'utente inserisce la sua pw e questa viene utilizzata come chiave per cifrare.

1.5 Cascade attack

Definizione: un attacco ne provoca altri direttamente. Supponiamo che C abbia violato una chiave di sessione (di autorizzazione) scaduta $authK$ che B condivise con A.

1.6 Limiti di Kerberos 4

1.6.1 Ambientali

- Uso obbligatorio di DES
- Dipendenza dal protocollo IP
- Codifica dei byte dei messaggi non definita
- Lifetime a 8 bit, fino ad un massimo di 21 ore

- Forward di autenticazione ad un altro host non previsto (cioè il trasferimento dell'accesso di un utente ad un altro terminale)
- I partecipanti sono denotatocon nome, istanza e reame con massimo 39 caratteri ciascuno e il carattere "." non è permesso.
- Autenticazione inter-realm dispendiosa, è necessario autenticarsi con ogni server di autenticazione del realm d'arrivo

1.6.2 Tecnici

- Doppia cifratura dei messaggi 2 e 4 superflua (provata da analisi formale)
- Utilizzo di cifratura PCBC, variante di DES vulnerabile
- Il server non mantiene una lista degli autenticatori non scaduti, ma già usati (vulnerabile a replay attack)
- Attacco alla password possibile perché la chiave usata per cifrare il messaggio 2 viene ottenuta algoritmicamente dalla password
- Replay di chiavi di sessione: B, finita la transazione con A, non deve accettare più materiale con quella servK
- MAC usato nell'implementazione del MIT diversa dall'originale

1.7 Kerberos 5

1.7.1 Cambiamenti

- Crittosistemi differenti: si concorda nei messaggi il crittosistema utilizzato
- Supportati differenti protocolli (non solo IP)
- Standardizzata la codifica dei byte
- Cambiamenti ai ticket per permettere il rimbalzo di credenziali ad altri host
- Gerarchia dei realms ad albero bilanciato
- Nomi dei partecipanti separati da punti (quello più a destra è la root)

1.7.2 Nuove features

- Tickets più complessi con più timestamps e il flag per il rimbalzo di credenziali
- Aggiunto il campo "Authorization data" allegato al ticket
- Pre-authentication data aggiunti per supportare alternative alle password
- Supportate le sottochiavi di sessione
- Aggiunto il sequence number (tramite timestamp o nonce)

1.7.3 To-do

- Supporto ai crittosistemi a chiave pubblica
- Pieno supporto alle smart-card
- Amministrazione remota
- Implementare propagazione del database
- Suite di validazione dell'implementazione
- Supporto a più applicazioni

1.7.4 Attacco a dizionario su Ka

Il problema più grande del protocollo è che Ka viene calcolata algoritmicamente dalla password, cioè è deterministica. L'idea per risolvere questo problema è far eseguire la decifratura del messaggio 2 da una smartcard, la quale pre-concorda dei parametri con l'AS per calcolare password random.

Il problema non è risolto completamente perché le smartcard devono essere protette da pin, il lettore della smartcard collegato al pc potrebbe essere compromesso, inoltre le credenziali decifrate al messaggio 2 restano nella cache della workstation. La soluzione migliore sarebbe eseguire l'intera sessione del protocollo su smartcard.

2 Smartcard

La potenza di calcolo nelle smartcard è migliorata negli ultimi anni, ma non tanto per cui questa tecnologia ha perso via via un po' interesse, a favore della la tecnologia NFC (es pagamenti), che è un chip di suo che garantisce collegamento senza fili. Le smartcard non hanno avuto l'esplosione di utilizzo per singolo utente che si poteva sperare. Inoltre, l'avvento del 5G ha spostato l'interesse verso la questione centrale delle eSim. *Perché è necessario avere un SIM legata così strettamente all'identità?*. Skype è un vero e proprio servizio nel senso web del termine di telefonia mentre il telefono mobile non lo è ancora, tant'è che contiene ancora la SIM legata all'identità. Da un lato c'è il produttore del telefono che fa solamente un terminale sul quale girano certi applicativi e chi si vuole autenticare lo fa autonomamente, mentre i gestori di telefonia sono legati ancora alla vecchia tecnologia con cui viene meglio gestire gli utenti. Dall'altro lato, anche giurisprudenza ha tentato di rendere più facile il cambio di gestore (legge Bersani). *Quale dovrebbe essere oggi il migliore mercato per le smartcard?* Stiamo andando verso la dematerializzazione della SIM. Se scompare la SIM scompare gran parte del mercato delle smartcard.

QUAL È IL MERCATO DI OGGI DELLE SMART CARD E IL MERCATO DI DOMANI? Le smartcard sono tante volte fraintese. Si pensa che una smartcard sia una protezione inoppugnabile per un segreto, ma prima delle smartcard c'erano le carte a banda magnetica. Quindi, se il chip fa una tale

differenza, tutte le carte prima erano tutte insicure? La banda magnetica, dal punto di vista dell'architettura di un calcolatore, è un supporto, una memoria, infatti una banda magnetica la si legge facilmente. Adesso il chip contiene anche una memoria, quindi ciò che era la banda magnetica lo è anche la smartcard, con l'aggiunta della CPU e quindi di calcolo e di conseguenza un gestore delle memoria.

Quando si parla di copia bit-bit questa non è impossibile, il problema però è interagire in qualche modo con la CPU, infatti la memoria è protetta dal microprocessore, quindi se dobbiamo clonare una carta dobbiamo andare a interloquire direttamente con il microprocessore. Anzitutto bisogna saperci parlare e sperare che il microprocessore capisca richieste del tipo "dammi in output tutta la memoria". Non tutte le carte si possono clonare allo stesso modo, infatti dipende da come è programmata la CPU.

Se la chiave a lungo termine dell'utente fosse registrata nella ROM, o la CPU è programmata con un routine di accesso totale alle ROM quella chiave sarà virtualmente protetta. Quindi la protezione offerta dalla smartcard verso la sua memoria non è una protezione inerentemente hardware ma software. Se il software fosse debole sarebbe facile leggere le informazioni come una banda magnetica, quindi tutto dipende dalla robustezza software con cui è programmata la CPU.

Quindi il destino della smartcard è in declino per i motivi legati agli smartphone (5G ed eSim).

2.1 Autenticazione dell'utente al sistema

Il problema dell'autenticazione dell'utente al sistema consiste nell'autenticare l'utente al sistema bancario per poter utilizzare la carta di credito, quindi non è esclusivamente utente-carta. Il protocollo spesso prevede l'inserimento di un PIN prima di procedere con la transazione.

Il PIN nelle carte non c'è sempre stato. I protocolli di utilizzo di una carta di credito a banda magnetica o di un bancomat prevedono l'utilizzo di un PIN. *Il PIN chi deve autenticare a chi?* I primi PIN erano registrati sulla carta magnetica.

Il PIN registrato in chiaro nelle carte a banda magnetica è debole, ma storicamente questa era la scelta. Gli autori, i partecipanti di questo protocollo sono più di uno, carta, utente, lettore locale della carta (in possesso dell'utente o ATM), server che ci stanno dietro. Quindi si tratta di un protocollo multiplayer. Quindi non si tratta di un'autenticazione uno ad uno ma di un insieme di fattori (player), al server centrale. Se anche l'ATM fosse alterato potremmo quindi alterare l'autenticazione dell'utente al sistema.

L'ISO/IEC 7816 è uno standard internazionale relativo alle carte di identificazione elettroniche a contatto, specialmente le smartcard.

2.2 Attacchi alle smartcard

2.2.1 Invasivi

Microprobing: si accede al chip, lo si smonta e lo si manipola. Vengono effettuati degli studi approfonditi su tutto il sistema per capirne il funzionamento. La memoria può essere anche rimappata ad-hoc.

2.2.2 Non invasivi

- Attacchi al software: attraverso vulnerabilità di algoritmi e protocolli
- Eavesdropping: monitoraggio di onde elettromagnetiche
- Fault induction: si adopera il chip in condizioni anormali (ad esempio con eccessivo calore)

3 Crittografia Visuale

La crittografia visuale è un'idea di Naor e Shamir del 1994. Consiste nel dividere un'immagine in due immagini detta **share**: chiave e crittogramma. Un attaccante non può ricavare informazioni da ciascuna. La sovrapposizione di chiave e crittogramma rivela l'immagine.

3.1 Applicazioni

Una possibile applicazione della crittografia visuale è per l'autenticazione utente-banca: la banca manda al cliente lo share chiave su vinile quindi la banca pubblica lo share crittogramma. Il cliente può quindi decodificare e leggere la password.

Un'altra possibile applicazione è l'e-voting, dove chi ha votato riceve uno share della ricevuta. Infatti, uno dei problemi del voto elettronico è il *Receipt Freeness*, ovvero che non ci siano ricevute. Nelle votazioni tradizionali, si torna a casa senza alcun tipo di ricevuta che indichi per chi abbiamo votato. Di contro, la ricevuta è la prima misura di verifica per l'utente. Ad esempio la ricevuta della raccomandata ha due valenze: dimostrabile in caso di conflitto e conferma dei dati importanti della raccomandata stessa. La prima parte, con il voto elettronico vogliamo toglierla, la seconda invece è auspicabile. Nel caso del voto elettronico non è possibile scindere questi due requisiti.

3.2 Codifica e decodifica

La decodifica è semplice, infatti basta sovrapporre i due share e l'occhio umano ricostruisce l'immagine.

La codifica è un po' più complessa. Data un'immagine in bianco e nero associamo due matrici 2×2 ad ogni pixel, in questo modo le due matrici forniscono i due share del pixel. Alternativamente si può immaginare che ciascun pixel

venga suddiviso in quattro sottopixel per sue volte. Così facendo per ogni pixel costruiamo i due share per l'immagine di partenza.

Nel caso delle matrici 2×2, ogni matrice è costruita in modo tale che abbia due sottopixel neri e due bianchi. La coppia di matrici è costruita in modo tale che la loro sovrapposizione dia nero totale oppure metà nero metà bianco cioè grigio. In questo modo vedendo l'immagine, l'occhio interpreta il nero totale come nero e il grigio come bianco. Quindi affinché l'occhio decodifichi un pixel nero le due matrici devono essere **complementari**, mentre per un pixel bianco, devono essere uguali. Questo consiste nell'applicare il crittoalgoritmo One Time Pad, che fa uso dell'operazione logica XOR. In questo modo lo schema di crittografia visuale di Naor e Shamir è sicuro quanto lo XOR. Dato uno share, per ogni immagine intelligibile esiste un altro share che sovrapposto al primo dia l'immagine.

L'algoritmo di codifica prende per ogni pixel dell'immagine, sceglie un bit a caso e associargli la matrice, in questo modo abbiamo ottenuto la chiave. Per la costruzione del crittogramma per ogni pixel nero dell'immagine, scegliere la matrice complementare della chiave del pixel, altrimenti la stessa matrice. Si crea quindi un'immagine b/n random grande quanto la data. Si associa la matrice [x][][x][] ad ogni pixel nero (0) e la matrice [][x][][x] ad ogni pixel bianco (1) così da ottenere lo share chiave. Successivamente si fa lo XOR fra l'immagine da celare e l'immagine random così da ottenere il crittogramma.

3.3 Extended Visual Crypto (EVC)

Dati n share, vogliamo che specifici sottoinsiemi (di qualunque cardinalità) di share ricostruiscano l'immagine, altri no.

4 Non ripudio

Definizione: *Disponibilità di evidenza inequivocabile che impedisca ad un soggetto di negare proprie azioni.*

Per inequivocabile intendiamo che sia dimostrabile in tribunale. Questo è garantito per mezzo della **firma elettronica**, che ha con un certo valore in Italia, e garantisce **equità** tra i due agenti coinvolti in modo che ottengano garanzie analoghe.

In un certo senso, il non ripudio non è tanto una misura di sicurezza ma una contromisura. Mentre le misure sono tipicamente preventive (l'autenticazione previene che qualcuno si spacci per qualcun altro, ecc), il non ripudio è una contromisura, perché non previene. Ad esempio, la telecamera non impedisce che qualcuno entri, non previene ma le smaschera qualora occorre, magari può svolgere il ruolo di deterrente, ma tecnicamente non impedisce l'azione. Allo stesso modo, le misure di non ripudio digitali, non prevengono eventuali falsità ma hanno come obiettivo lo smascherare eventuali falsità, in genere sono partecipazione ad una transazione (ricezione o invio di un messaggio). Tipicamente,

i giuristi direbbero che l'autenticazione è una misura ex-ante cioè che anticipa, e il non ripudio è una misura ex-post, a posteriori. Una misura ex-post non è una misura.

L'autenticazione non implica il non ripudio. E' vero che l'interlocutore si è autenticato alla chat, ma non vuol dire che il sistema abbia messo qualche evidenza crittografica che dall'altra parte c'è effettivamente quella persona. Se ho autenticazione devo ancora lavorare per avere non ripudio, il viceversa invece sussiste. Questa evidenza deve essere inequivocabile ed equa. Se si tratta di un protocollo tra due agenti, allora ambedue devono avere la medesima evidenza. Se il mezzo fosse del tutto affidabile non potremmo imputare eventuali mancanze e dire di non aver ricevuto qualcosa che invece abbiamo ricevuto. Se un partecipante fosse onesto il problema sarebbe molto più facile. Il caso roseo è piuttosto improbabile. Il caso più realistico è quello in cui ambedue condizioni siano false.

Anche per il non ripudio è importante definire il corretto modello di attaccante. Dolev-Yao non è il modello più indicato per questo tipo di protocollo, perché gli interlocutori si fidano uno degli altri e c'è un attaccante che si intromette, mentre in General-Attacker nessuno si fida di nessuno e quindi gli aspetti di non ripudio vengono meglio espressi.

Tre problemi del non ripudio nel mondo elettronico:

1. Compravendita
2. Delega
3. Email

Sono problemi molto simili ma in ambiti diversi.

I fattori determinanti nel non ripudio sono **l'affidabilità del mezzo** ("*non l'ho mai ricevuto*") e **l'onestà dei partecipanti** ("*ho quello che mi serve, chiudo*" oppure "*e se gli mando un siffatto messaggio?*"). Tutte le quattro combinazioni sono possibili.

4.1 Compravendita

Scenario:

- **Venditore**: "*Ti ho mandato la merce. Dov'è il denaro?*"
- **Acquirente**: "*Ti ho mandato il denaro. Dov'è la merce?*"

Precondizioni:

- Agenti generici A e B
- PKI
- Messaggio m cruciale per la compravendita

- TTP
- Aggiuntive (a seconda del caso)

L'obiettivo finale è garantire **equa compravendita**, ovvero: A spedisca un messaggio m a B in modo tale che A ottenga evidenza che B l'abbia ricevuto se e solo se B ottenga evidenza che A l'abbia spedito. In altri termini, nessuno dei due ha un vantaggio sull'altro.

Esempio 1.
Precondizioni: mezzo affidabile e agenti onesti.

1. $A \longrightarrow B \ : \ f_{nro}, B, m, Sign_A(f_{nro}, B, m)$
2. $B \longrightarrow A \ : \ f_{nrr}, A, m, Sign_B(f_{nrr}, A, m)$

Alla recezione del messaggio 1, B lo conserva. Siccome il mezzo non è affidabile come facciamo a garantire che il messaggio che parte arrivi a destinazione? Si potrebbe utilizzare un ACK di conferma. Se il messaggio non arriva a destinazione, perché il mezzo non è affidabile, il protocollo è terminato senza problemi senza che il suo obiettivo venga sovvertito. Perché nessuno di due ha evidenza. Supponiamo che il messaggio 1 va a buon fine, siccome B è onesto, B prodiga ad A l'evidenza che può servirle (firma di B su m su un flag che esplicita il senso di questo certificato).

[DA COMPLETARE (?)]

Esempio 2
Precondizioni: mezzo affidabile e agenti disonesti.

1. $A \longrightarrow TTP \ : \ f_{nro}, TTP, B, m, Sign_A(f_{nro}, TTP, B, m)$
2. $TTP \longrightarrow B \ : \ f_{nrs}, A, B, m, Sign_A(f_{nrs}, A, B, m)$
3. $TTP \longrightarrow A \ : \ f_{nrd}, A, B, m, Sign_B(f_{nrd}, A, B, m)$

In questo caso gli agenti sono disonesti, di conseguenza un TTP si occuperà di trasmettere sia il messaggio che le ricevute ad entrambi i partecipanti.

Esempio 3
Precondizioni: mezzo inaffidabile e agenti onesti.

1. $A \longrightarrow B \ : \ f_{nro}, B, m, Sign_A(f_{nro}, B, m)$
2. $B \longrightarrow A \ : \ f_{nrr}, A, m, Sign_A(f_{nrr}, A, m)$
3. $A \longrightarrow B \ : \ f_{ack}, Bm, Sign_B(f_{ack}, B, m)$

In questo caso il canale è inaffidabile, di conseguenza A manda il messaggio 3 per realizzare l'equità.

4.2 Strategia a rilascio posticipato

Si basa sui seguenti punti:

- Inizialmente dare il crittotesto al ricevente
- Se il ricevente è interessato a decodificare il crittotesto deve continuare la sessione
- Mentre continua da evidenza di partecipazione
- Infine dare al ricevente la chiave

Tentativo
Precondizioni: mezzo inaffidabile e agenti disonesti.

1. $A \longrightarrow B \ : \ f_{poe}, B, c, Sign_A(f_{poe}, B, c)$
2. $B \longrightarrow A \ : \ f_{acp}, A, Sign_B(f_{acp}, A, c)$
3. $A \longrightarrow B \ : \ f_{nro}, B, k, Sign_A(f_{nro}, B, k)$
4. $B \longrightarrow A \ : \ f_{nrr}, A, Sign_B(f_{nrr}, A, k)$

Ma B manderà l'ultimo messaggio? Al messaggio 1 B non ha vantaggio perché ha un crittotesto che ovviamente non riesce a comprendere. Quindi B intende partecipare e costruisce il messaggio 2, ovvero è d'accordo a proseguire, quindi invia il messaggio 2 dicendo che effettivamente che ci sta. A invia al messaggio 3 la chiave k e alla recezione di 3 B può accedere al messaggio c in chiaro per mezzo di k. Perché ad A non bastava il messaggio 2? A ha bisogno del messaggio 4, mentre a B interessa il messaggio 3, e quindi può non mandare 4. Quindi il protocollo non garantisce equità, ovvero nel caso in cui B non manda il messaggio 4 a A. Il protocollo non va bene quando B al messaggio 3 **ha un vantaggio** su A e decide di chiudere il protocollo con un vantaggio. Questo protocollo non usa strategia progettuale per arginare la possibilità di disonestà degli interlocutori.

4.3 Protocollo Zhou-Gollmann

È un protocollo che garantisce equa compravendita nella situazione reale implementando la strategia a rilascio posticipato ricorrendo ad un TTP.
Siano:

- L (lable/link). Collegamento alla risorsa, che servirà per collegare i vari pezzi di evidenza crittografica tra loro ovvero l'indicazione di collegamento tra chiave e crittotesto.
- $NRO = Sign_A(f_{nro}, B, L, c)$ evidenza di origine, firmata dal mittente (specificata dal flag) relativa all'interlocutore
- $NRR = Sign_B(f_{nrr}, A, L, c)$ evidenza di ricezione

- $sub\_k = Sign_A(f_{sub}, B, L, k)$ evidenza di aver sottoposto k all'attenzione della controparte fidata
- $con\_k = Sign_{TTP}(f_{con}, A, B, L, k)$ conferma su k data dal TTP, conferma che esprime gli elementi salienti della sessione

Protocollo

1. $A \longrightarrow B \ : \ f_{nro}, B, L, c, NRO$
2. $B \longrightarrow A \ : \ f_{nrr}, A, L, NRR$
3. $A \longrightarrow TTP \ : \ f_{sub}, B, L, k, sub\_k$
4. $B \xleftarrow{FTP} TTP \ : \ f_{con}, A, B, L, k, con\_k$
5. $A \xleftarrow{FTP} TTP \ : \ f_{con}, A, B, L, k, con\_k$

Nel messaggio 1 A manda a B NRO. A questo punto B ha un leggero vantaggio su A perché ha un crittotesto che non riesce a decifrare. Se B ci sta al protocollo, allora invia ad A l'intenzione di continuare. Quindi al passo 2 c'è una parità, ma basata su crittotesto. Successivamente (passo 3) A manda un messaggio a TTP, firmando una sotto chiave. TTP allora può verificare la firma su sub_k e se tutto funziona può rendere k disponibile al pubblico tramite la sua firma digitale. Questa firma digitale di TTP, che convalida k, è con_k. Gli ultimi due passi, 4 e 5, sono praticamente uguali. E Sono gli unici passi in assoluto in cui la freccia è al contrario. Questa freccia in realtà `FTP get`. A e B infatti "scaricano" la chiave da TTP, infatti TTP rende disponibile con_k e non deve inviare niente. Il motivo dell'utilizzo di FTP è puramente storico. Infatti al tempo FTP era lo strumento più comune per la condivisione remota di file, anche se FTP non è un protocollo di sicurezza in quanto non c'è alcun tipo di cifratura.

Il protocollo garantisce **equità**, infatti per vincere eventuali dispute su B, A (e viceversa) cosa servirebbe? C'è interesse da parte di tutti ad arrivare all'ultimo step del protocollo. Infatti, nessuno ha interesse a fare quit prima in quanto farlo non garantirebbe nessun vantaggio. Alla fine del protocollo A ha NRR e con_k. Mentre B ha NRO e con_k. Esiste quindi equo recapito con questo protocollo e non c'è un modo per violare questa proprietà. Se B dice di non aver mai ricevuto m da A, a questo punto A può esibire NRR e mostra che B ha firmato il crittotesto abbinato ad L e può esibire con_k che dimostra che TTP ha fatto endorcing con la firma digitale della chiave k abbinata con L. B avrebbe potuto scaricarsi con_k allo stesso modo, perché il protocollo è noto e TTP è affidabile. Se B possiede con_k allora può ottenere k come abbinata in maniera affidabile sancita dal TTP al link L. B stesso, esibendo NRR, ha visto il crittotesto e l'ha abbinato al link L. Ciò significa che B conosce c, k e sa che sono abbinati tra loro. Quindi B avrebbe potuto decifrare c per mezzo di k. Nella risoluzione di queste dispute TTP non ha avuto bisogno di partecipare, quindi la disputa la possono risolvere direttamente A e B.

È stato osservato che TTP deve fare stato altrimenti il protocollo sarebbe vulnerabile verso un attacco di replica. Il protocollo fa un'enorme assunzione, contraria al principio di difesa in profondità, in modo che la freshness sia controllata e generata esternamente, in particolare fatta dall'unico partecipante affidabile.

5 PEC

La Posta Elettronica Certificata in Italia ha valore legale ed è la versione digitale della raccomandata con ricevuta di ritorno. In Italia solo un certo numero prefissato di enti possono agire come gestori di servizi accreditati per fare la PEC. Per eseguire il protocollo PEC servono quindi più enti accreditati per garantire il servizio, basando difatto il tutto sulla pura fiducia. Nessuna viene usata alcuna misura tecnologica o protocollo di sicurezza che certifichi che l'email sia partita e sia arrivata. Di fatto la fiducia che poniamo nel TTP di Zoul-Golmann è una fiducia pari a quella che poniamo ad un autorità di certificazione, non che certifichi solamente la posta elettronica. La PEC è esclusivamente una **certificazione** da parte del gestore di avere visto quella posta. Se si pone fiducia nel certificato che dice che A ha inviato a B. Se fossimo in un mondo di totale trust non ci servirebbero misure di sicurezza. Con le nostre tecnologie non azzeriamo gli atti di fede. Questo è diverso da avere misure di sicurezza che coinvolgano una partecipazione minima di un'autorità. Nel caso dei servizi di PEC la partecipazione non è leggera, ma è assoluta. L'autorità di certificazione della posta (gestore della posta) ha una fiducia cieca per lo stato italiano. Lo stato riconosce che Aruba può sostenere, portare avanti il servizio e tutti quanti prendono questa fiducia. Invece, il protocollo di Abadi non prescinde da un'autorità, ma la utilizza in maniera leggera. Solo semplici verifiche di hash e firme digitali, ovvero assunzioni molte più deboli rispetto a quelle che facciamo in Italia su Aruba.

5.1 Chi firma che cosa

L'ente non mette solo il timbro in un passaggio, ma gestisce tutto il processo. Non c'è sicurezza end-to-end, ma è una scelta progettuale. La PEC non è verificabile esternamente ma solo tra i gestori rispettivi di A e B, perché non c'è la firma di A e B.

6 Protocollo di Abadi et al.

Abbiamo presentato questo protocollo con una valutazione della PEC in Italia. Abbiamo convenuto che la PEC è fortemente basata sull'esistenza di autorità autorizzate per la vendita del servizio di fiducia, relativamente al recapito dei messaggi di posta. Sostanzialmente, una PEC funziona con dei protocolli, come la mail normale ma con l'aggiunta di alcune firme digitali che in particolare

confermano la ricezione dell'email di un mittente da parte del gestore di posta del ricevente.

Questo protocollo ha una forte trovata pubblicitaria che consiste di non avere bisogno di una PKI. Se avessimo avuto un PKI tutto quello che segue sarebbe stato inutile, perché PKI ci garantisce un'infrastruttura affidabile per gestire certificati. Questo protocollo utilizza TLS, con l'obiettivo di avere una forma di equo recapito (debole). Ovvero garantire che il ricevente legga la mail se e solo se il mittente riceve la ricevuta di ritorno. Simile alle raccomandate con la ricevuta di ritorno (e anche WhatsApp ha un sistema simile).

Possiamo mandare una raccomandata per conto di qualcun altro? Si. Possiamo ritirare una raccomandata intestata ad un nostro familiare? No, a meno che non ci sia la delega da parte del vero destinatario della raccomandata. Quindi progettualmente in fase di spedizione non c'è autenticazione del mittente, ma in fase di ricezione in qualche modo si. Questo significa che il mittente non si autentica ed è coerente con la definizione di equo recapito. Per questo viene definita *forma debole* in quanto non c'è nessun tipo di vincolo su attività del mittente. Come per la raccomandata reale, il ricevente ottiene una mail e manda un ricevuta di ritorno al mittente, ma il ricevente non ha un'evidenza crittografica di chi sia il mittente. La PEC italiana ce l'ha sempre in fiducia del gestore. In sintesi, questa definizione è coerente e la proprietà di sicurezza che la raccomandata tradizionale intende raggiungere, ovvero è debole nel senso che non sembra esserci alcun binding nei confronti del mittente.

È possibile comunque irrobustire la definizione appena data, ovvero: Il ricevente legga l'email e ottiene evidenza che la mail provenga dallo specifico mittente, se e solo se il mittente riceva la ricevuta di ritorno (equo recapito forte). Ciò significa che il ricevente ha ottenuto evidenza che la mail provenga da quel mittente, oltre autenticazione quindi c'è non ripudiabilità di quel mittente. Questa definizione è forte per almeno due ordini di grandezza in più, quindi non solo autenticando il mittente, ma ottenendo pure l'evidenza su di esso.

Con un protocollo di questo genere, che gestisce il trasferimento di un messaggio, svanisce il senso della firma grafometrica tradizionale sulla lettera, in quanto la firma era un tentativo di autenticare quel messaggio. A questo punto nel mondo digitale il senso è completamente svanito perché sarà il protocollo a dare evidenza di autenticazione del mittente. Questo protocollo costruisce evidenza digitale.

Il protocollo di Abadi ottiene solo il primo livello della proprietà, quindi equo recapito debole.

Siano:

- $h_S = Hash(q, r, c)$
- $h_R = Hash(q', r', c')$
- $S2TTP = \{S, k, R, h_S\}_{pubEKTTP}$

- $DR = Sign_{TTP} S2TTP$

dove q ed r sono due parametri legati fra loro dalla funzione preconcordata fra mittente e ricevente chiamata `ack`. s sta per *sender* e r sta per *receiver*. Questi, messi all'interno dell'hash consentono di autenticare chi ha messo quei valori all'interno dell'hash. Il $S2TTP$ serve in quanto, non essendoci una PKI il ricevente non possiede una chiave privata di firma, quindi il massimo che si può fare è avere una garanzia da parte del TTP. Il TTP è abbastanza cieco, si limita a mettere la firma sulla busta digitale. In ogni caso la proprietà di equo recapito debole non è toccata da questa potenziale debolezza.

Protocollo

1. $S \longrightarrow R \ : \ TTP, c, q, S2TTP$
2. $R \xrightarrow{SSL} TTP \ : \ S2TTP, pwd, R, h_R$
3. $TTP \xrightarrow{SSL} R \ : \ k, h_R$
4. $TTP \longrightarrow S \ : \ DR$

Il protocollo per se è piuttosto ermetico. Il mittente dice al ricevente di parlare con lui su c (strategia a rilascio posticipato) per mezzo di TTP, mandando la query, che viaggia in chiaro (non importa che la query rimanga confidenziale, l'importante è che non si esposta in chiaro la coppia query-response). S manda la query in chiaro e costruisce $S2TTP$ codificata con la chiave pubblica di TTP, ottenendo così confidenzialità. Questo messaggio può essere comunque alterato, infatti c potrebbe essere alterato, ma in tal caso il protocollo non andrebbe a buon fine. Qualsiasi messaggio alterato potrebbe a non far andare a buon fine il protocollo. Ad un certo punto R, quando riceve il messaggio alterato o meno, inoltra al TTP il certificato, la propria pwd e H_R. SSL c'è sostanzialmente per proteggere la pwd. R non fa altro che prendere $S2TTP$ e inoltrarlo (se è stato modificato inoltrerà quello), così come q. In generale ciò che R ha tra le mani è q'. Si evince che il protocollo dice che il mittende e ricevente condividono una password con TTP. Qui si avverte l'utilizzo della password di R (messaggio 2) ma non si è visto l'utilizzo della password di S.

Potrebbe accadere che H_R è uguale ad H_S che si trova su $S2TTP$ ma non è detto che questo accada sempre. Quando il messaggio 2 viene ricevuto da TTP, confronta H_R con H_S. Quindi alla ricezione del messaggio 2 il TTP prende H_S, contenuto dentro $S2TTP$ prende H_R appena ricevuto e li confronta. S ed R hanno saputo calcolare la response alla precisa query q quindi ambedue conoscono la funzione. Se H_R ed H_S corrispondono, allora S e R si sono autenticati tra di loro e non c'è stata alcuna alterazione.

Se invece H_R ed H_S risultano distinte, significa che o c'è stata una modifica/alterazione in transito oppure S ed R non sono chi dicono di essere. R in particolare non ha saputo calcolare la response giusta. Se quindi il controllo tra i due hash fallisce, TTP che è fidato fa abort. Si comincia a vedere come TTP sia partecipa in maniera leggera perché non fa altro che fare un confronto. In

caso affermativo TTP estrae la chiave k da $S2TTP$, nel messaggio 3, insieme ad una copia di H_R. Si capisce quindi perché il messaggio 3 ha bisogno di SSL. Questo protocollo è più recente di Zouh-Gollmann in cui si vedeva la chiave k in chiaro.

Ancora una volta, un po' come Zouh-Gollmann i messaggi 3 e 4 vedono come soggetto fondamentale TTP, in quanto è lui che manda in contemporanea. Se si permette ad R di leggere la mail allora si permette ad S di avere la ricevuta di ritorno. Dal punto di vista di equità, si riduce a questa osservazione che il recapito della chiave necessaria per aprire la mail è fatta in concomitanza al recapito al mittente della ricevuta di ritorno, in concomitanza perché è demandato al TTP che si assume essere coerente con questa premessa di fare tutte e due cose oppure nessuna.

Ci potrebbe essere il problema di resilienza del canale, ad esempio il fatto che TTP mandi il messaggio 3 non è detto che questo arrivi e uguale anche per il 4. Si potrebbe pensare allora alla stessa strategia di Zouh-Gollmann.

R ha già dovuto usare la propria password nel messaggio 2, nel senso che R si è dovuto autenticare con TTP prima che questo gli mandasse la chiave. Una cosa è il controllo su H_S e H_R per desumere che gli interlocutori che si conoscono fra loro per mezzo della funzione preconcordata. Ma prima TTP vuole autenticalo.

Il protocollo garantisce l'equo recapito debole? Si, ovvero il ricevente riceve la mail se e solo se il mittente riceve una ricevuta di ritorno, che è valida ed indicativa su chi abbia ricevuto cosa. La ricevuta di ritorno vincola il ricevente R perché TTP l'ha voluto autenticare con la password nel messaggio 2 (parallelo con il protocollo postale).

Alla fine il protocollo da una ricevuta di ritorno al mittente, nel senso che inchioda il ricevente e al mittente basta perché la ricevuta non inchioda S, perché S non si è mai autenticato!

Ma S, se il protocollo va a buon fine, si autentica con R? Per ipotesi R ed S condividono una funzione `ack` segreta. Quando TTP alla ricezione del messaggio 2 confronta H_R con H_R significa che si sono autenticati tra loro ma questa verifica l'ha fatta TTP nel messaggio 2 ed R non se n'è ancora accorto. Quindi da un lato S ed R si autenticano tra loro, perché i due hash sono uguali, però da un lato c'è il fatto assoluto i due si autenticano da un lato [01:10:35] Il momento in cui il dato sull'autenticazione è disponibile ad R è alla ricezione del messaggio 3.

Supponiamo che R imbrogli e dica di non aver mai ricevuto questa mail da S. S allora dichiara di avere la ricevuta di ritorno con la firma digitale. Allora ci sono due strade:

- Si richiede la partecipazione del TTP, affinché TTP possa decifrare il messaggio S2TTP (strada difficile)
- S, dipendentemente dalle proprietà dello schema crittografico, potrebbe fornire i parametri di input fornendo S, k, R, H_S e cifrando con la chiave pubblica di TTP otteniamo il risultato di $S2TTP$. Così facendo S riesce a smascherare la falsità dell'affermazione di R.

C'è questo passaggio, dovuto al fatto che il contenuto della firma è esso stesso un crittotesto. L'equo recapito forte è uguale all'equa compravendita del protocollo Zouh-Gollmann.

6.1 Protocollo Crispo

Il protocollo Crispo si occupa di garantire l'**equa delega**.

Definizione: *Il grantee riceve evidenza che il grantor gli ha dato diritto su* Ω *se e solo se il grantor riceva evidenza che il grantee ha accettato la responsabilità su* Ω

Nota: il grantee non ha nessun obbligo di eseguire Ω.

Prima di tutto è necessario definire uno schema di chiavi asimmetriche in cui ogni coppia ha un utilizzo diverso.

Firma	priSK	pubSK
Delega	priDK	pubDK
Accettazione	priAK	pubAK
Esercizio	priEK	pubEK

Per semplicità nella lettura dei messaggi, verrà omessa la parte in chiaro perché è identica al corpo della firma.

1. $G \longrightarrow g \ : \ Sign_{priSK_G}(G, g, \Omega, pubDK_G)$
2. $g \longrightarrow G \ : \ Sign_{priSK_g}(g, \Omega, pubAK_g, pubEK_g)$
3. $G \longrightarrow g \ : \ Sign_{priDK_G}(g, G, \Omega, pubDK_G, pubEK_g, pubAK_g)$

Una volta ricevuto il messaggio 3, g può esercitare Ω esponendo il token di delega: $Sign_{priAK_g}(Sign_{priDK_G}(g, G, \Omega, pubDK_G, pubEK_g, pubAK_g))$.

6.1.1 Risoluzione dispute

Se il grantor nega di aver delegato il grantee, allora il grantee mostrerà il token di delega.

Se il grantee nega di aver accettato la responsabilità, allora il grantor mostrerà il messaggio 2.

Se il grantee nega di aver esercitato Ω, il grantor mostrerà il messaggio 2 e il token di delega presentato all'end-point.

7 Data Protection

Privacy: diritto alla segretezza dei dati.

7.1 Dati personali

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

Particolarmente importanti sono:

- i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

- i dati rientranti in particolari categorie: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;

- i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti Le parti in gioco:

- **Interessato** è la persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l"interessato" (articolo 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);

- **Titolare** è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento (articolo 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);

- **Responsabile** è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati (articolo 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate

condizioni, designare un altro soggetto c.d. "sub-responsabile" (articolo 28, paragrafo 2).

7.2 Data protection

Definizione: processo di salvaguardia delle informazioni importanti dalla corruzione, compromissione o perdita.

In sintesi, è un processo per la difesa da un data breach.

7.2.1 Mettere in sicurezza un'azienda

Amministratore di sistema: in ambito informatico personale finalizzato alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Titolari del trattamento (Provvedimento del Garante Privacy)

4.1 Valutazione delle caratteristiche soggettive *L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.* Come si può valutare l'affidabilità del soggetto?

4.2 Designazioni individuali *La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.*

4.3 Elenco degli amministratori di sistema *Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.* L'azienda deve prendere la lista e la deve rendere nota e conoscibile, quando l'amministratore si occupa di sistemi sul quale ci sono dati personali. Chiunque lavora in un'azienda deve essere messo nelle condizioni di conoscere chi sono gli amministratori di sistema, nel caso di *outsourcing*.

4.4 Verifica delle attività *L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.*

4.5 Registrazione degli accessi *Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le*

registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

7.3 Decreto legislativo 196/03

7.3.1 Autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata **conosciuta** solamente dal medesimo oppure in un dispositivo di autenticazione in **possesso** e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una **caratteristica biometrica** dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o piu' credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati e' prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando e' prevista dal sistema di autenticazione, e' composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed e' modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave e' modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Nota: Informativa da far firmare all'impiegato e importanza della formazione per istruire il personale. Una sessione di trattamento: qualunque momento di trattamento (anche istantanea). Le soluzioni a queste problematiche sono di natura tecnica, per esempio il blocco schermo con password, oppure organizzative.

10. Quando l'accesso ai dati e agli strumenti elettronici e' consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessita' di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali e' organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Nota: nasce la figura del **fiduciario**, incaricato della custodia delle copie delle credenziali dell'incaricato.

7.3.2 Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

Nota: un profilo amministrativo va predeterminato.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. 14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

7.3.3 Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Nota: oltre alla verifica deve essere possibile produrre la lista per profili autorizzativi.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento e' almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Note: il salvataggio si riferisce al backup (RTO). 23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

7.3.4 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

7.3.5 Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per

prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione e' programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

7.3.6 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalita' di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identita' genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico e' cifrato.

7.3.7 Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

7.3.8 Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari e' controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

7.4 GDPR

7.4.1 Capo II - principi

Definizioni (articolo 4):

- **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- **Profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- **Pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Principi applicabili al trattamento di dati personali (articolo 5).

1. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (limitazione della finalità);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (limitazione della conservazione);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali,

compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (responsabilizzazione, principio di accountability. Migliore traduzione sarebbe imputabilità).

Liceità del trattamento (articolo 6).
1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Condizioni per il consenso (articolo 7).

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale

contratto.

Trattamento di categorie particolari di dati personali (articolo 9).

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

7.4.2 Capo III - Diritti dell'interessato

Diritto di accesso dell'interessato (articolo 15).

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto op-

pure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Diritto di rettifica (articolo 16).

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto alla cancellazione (diritto all'oblio) (articolo 17).

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.

Diritto alla portabilità dei dati (articolo 20).

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

Diritto di opposizione (articolo 21).

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (articolo 22).

7.4.3 CAPO IV - Titolare del trattamento e responsabile del trattamento

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (articolo 25).

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della

natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Sicurezza del trattamento (articolo 32).

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Notifica di una violazione dei dati personali all'autorità di controllo (articolo 33).

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Comunicazione di una violazione dei dati personali all'interessato (articolo 34).

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33,

paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Valutazione d'impatto sulla protezione dei dati (articolo 35).

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

8 Analisi formale

L'analisi formale fornisce garanzie matematiche sulla correttezza dei protocolli. Esistono vari approcci per l'analisi formale di protocolli:

- Logica di autenticazione
- Process calculi
- Linguaggi ad-hoc
- Induzione matematica

Strumenti principali per l'analisi dei protocolli:

- **Model checking** (enumerazione degli stati): alla ricerca di attacchi. Specifica il sistema come insieme di **stati**, dove ogni stato può essere inteso come una **fotografia** del sistema in esecuzione. Costruisce una macchina

a stati finiti, cercando attacchi in tutti gli stati, per proprietà negata. Inoltre offre supporto ai vari approcci di analisi (es. process calculi).

- **Theorem proving**: cerca di provare la correttezza, per esempio considerando il sistema per induzione. Offre supporto per induzione matematica e linguaggi ad-hoc.

Definizioni:

- **Traccia**: lista di eventi, ovvero una semplificazione del continuo.
- **Liveness**: esiste almeno uno stato su cui c'è una certa proprietà. L'attacco è una proprietà di liveness.
- **Safety**: per tutti gli stati una certa proprietà non c'è. L'assenza dell'attacco è una proprietà di safety.

Nesso tra eventi e conoscenza.