12 febbraio 2019

Tavolo tecnico interoperatore ex delibera 396/18/CONS

Processo di Assurance:
Criptazione dati sensibili

Agenda

- Premessa
- Definizione delle informazioni sensibili
- Criptazione delle informazioni sensibili
- Fasi di progetto
- Allegato 1: Tracciato Record di apertura segnalazione
- Allegato 2: GUI di apertura segnalazione
- Allegato 3: Tracciato Record di sospensione del TT e di esito collaudo da parte OAO
- Allegato 4: Osservazioni degli OAO e riscontri TIM

Premessa

- In relazione a quanto previsto dalla **delibera 396/18/CONS** pubblicata il 2 ottobre 2018, AGCom ha istituito un tavolo tecnico con TIM e gli OAO che:
  - si è riunito il 19 novembre, il 4 ed il 17 dicembre 2018 ed il 18 gennaio u.s.
  - ha individuato le modalità per introdurre «un **sistema di criptazione delle informazioni sensibili**»
- Il presente documento riporta le **modalità concordate** tra gli Operatori per realizzare, con riferimento al processo di Assurance, la **criptazione dei dati sensibili**.

Definizione delle informazioni sensibili

- Partendo dalle informazioni previste dai *tracciati record* (**di seguito TR**) *e dalle Interfacce Grafiche Utente* (**di seguito GUI**) attualmente utilizzate dagli OAO per aprire una segnalazione di guasto sulle linee dei propri clienti sulle quali è attivo un servizio wholesale acquistato da TIM (di cui all'Allegato 1), sono state individuate le informazioni dalle quali direttamente o indirettamente è possibile contattare il cliente dell'OAO
- Tali informazioni, riportate nella tabella seguente, vengono definite **sensibili** e sono oggetto di criptazione secondo le modalità di seguito descritte

Tipo di informazione	Grado di riservatezza
1. Anagrafica cliente	●
2. Nr. recapito e recapito alternativo	●
3. Campo note/disponibilità	●

● Informazioni sensibili

Criptazione delle informazioni sensibili (1/5)

Di seguito si riporta la modalità tecnica per realizzare la criptazione delle informazioni sensibili:

1. OAO compila il TR/GUI inserendo:
   - il numero di telefono di recapito del cliente
   - il numero di recapito alternativo
   - l'anagrafica del cliente

   La denominazione dei campi del TR che contengono tali informazioni per i servizi wholesale dati e fonia è riportata in Allegato 1.
2. Nei TR/GUI attualmente in campo utilizzati dagli OAO per l'apertura dei TT sui servizi ULL, ULL+NP, Shared access, SLU, WLR, Easy IP ADSL, CPS e NP non è presente il campo recapito alternativo del cliente
3. Ipotesi 1: Verrà introdotto nel TR dei servizi ULL, ULL+NP, Shared access, SLU, WLR, Easy IP ADSL, CPS e NP il campo recapito alternativo del cliente; ciò per evitare che l'OAO inserisca tale informazione in altri campi del TR qualora ritenga necessario fornire a TIM più di un recapito telefonico del suo cliente finale. Per tali servizi il campo recapito alternativo dei TR sarà opzionale.

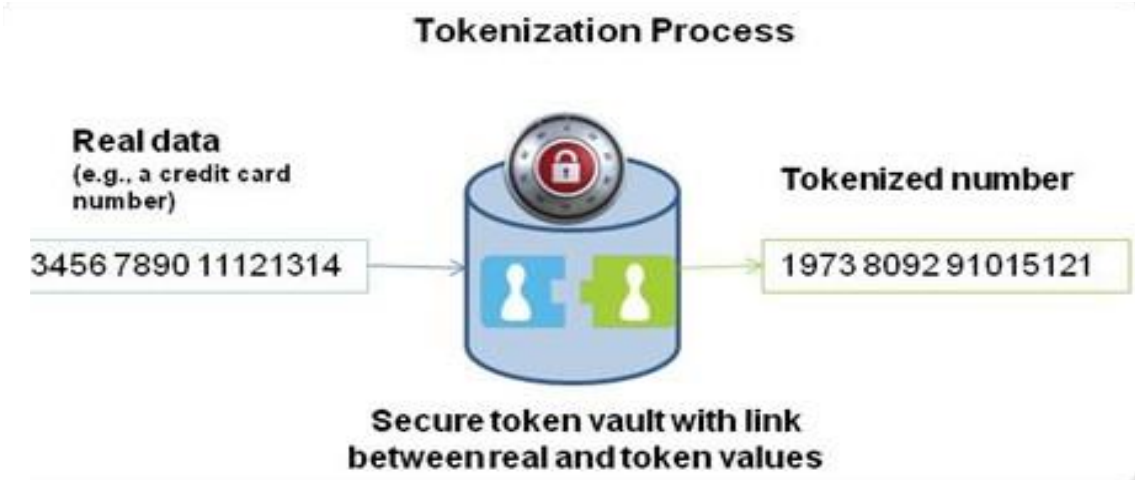
   Ipotesi 2: Verranno mantenuti gli attuali TR con possibilità di inserimento di recapiti nel campo note.

Criptazione delle informazioni sensibili (2/5)

5. TIM cripta le informazioni sensibili appena «entrano» nei sistemi TIM
6. Per le GUI l'OAO, ma non TIM, avrà la possibilità di visualizzare in chiaro le informazioni sensibili anche a seguito della relativa criptazione da parte di TIM
7. La criptazione consiste nella sostituzione di ciascuna delle informazioni sensibili con un identificatore unico detto **token**
8. Il token è memorizzato su **un nuovo DB** protetto, che è esterno ai sistemi di assurance di TIM
9. Il **nuovo DB**, correlato delle più recenti e innovative misure di sicurezza per garantire la riservatezza delle informazioni sensibili, conterrà l'associazione tra le informazioni sensibili del cliente e il token
10. Sui sistemi di assurance visibili a TIM il dato non sarà più presente in chiaro ma al suo posto sarà visualizzato il token
11. Il nuovo DB sarà interrogato in ottica need to know dai sistemi che utilizzeranno dati criptati per l'esecuzione della lavorazione.

Criptazione delle informazioni sensibili (3/5)

12. L'accesso al nuovo DB per poter estrarre più utenze sarà permesso:
    - al solo personale IT che svolge attività di sviluppo ed esercizio del sistema
    - per attività di sviluppo e manutenzione del sistema, per gestione reclami, per contenziosi e analisi di sicurezza.
13. Tutti gli accessi applicativi al nuovo DB saranno tracciati sui log di sistema con indicazione dell'utente che ha effettuato l'accesso, dell'operazione svolta e del dato interrogato



Criptazione delle informazioni sensibili (4/5)

14. L'OAO non dovrà inserire nei campi:
    - NOTE_DISP del TR dei servizi dati
    - DIAGNOSI del TR dei servizi dati
    - DIAGNOSI_OLO del TR dei servizi fonia
    - Diagnosi Cliente delle GUI dei servizi fonia
    - Analisi HD OLO/ISP delle GUI dei servizi dati

    le informazioni sensibili (cfr Allegati 1 e 2). Qualora lo facesse, qualsiasi misura di criptazione, fatto salvo quanto riportato nel punto 15, perderebbe la sua validità in quanto il dato criptato sarebbe disponibile in chiaro sul campo note;

15. TIM non effettuerà alcuna sovrascrittura di eventuali dati anagrafici del cliente inseriti dall'OAO nei campi citati nel punto 14. Qualora OAO inserisse impropriamente tale informazione in tali campi queste rimarranno in chiaro;

16. Ipotesi 1: TIM attuerà soluzioni di controllo per minimizzare la perdita di validità della criptazione delle informazioni sensibili nel caso in cui l'OAO dovesse inserire nei campi di cui al punto 14 i recapiti telefonici. In particolare su tali campi TIM utilizzerà algoritmi di pattern matching e di riconoscimento di sequenza di numeri con determinate caratteristiche per «intercettare» la presenza di eventuali numeri telefonici. Tutti i numeri telefonici intercettati dall'algoritmo, ivi inclusi eventuali riferimenti telefonici dell'OAO, verranno sovrascritti rendendoli inutilizzabili.

    Ipotesi 2: TIM non attuerà alcun controllo ed alcuna sovrascrittura sui contenuti dei predetti campi.

Criptazione delle informazioni sensibili (5/5)

17. Nel TR denominato **«Suspend»** usato da TIM per comunicare agli OAO la sospensione della lavorazione su una sua segnalazione di guasto, TIM NON effettuerà alcuna sovrascrittura di eventuali informazione relative al cliente finale recuperate dal personale TIM in fase di lavorazione della segnalazione (cfr. Allegato 3)
18. Nei TR denominati **«setTestingFailureDataService»** e «**setTestingFailureUnbundlingService»** utilizzati dall'OAO per comunicare a TIM l'esito negativo del collaudo da lui effettuato su una sua segnalazione di guasto dichiarata risolta da TIM e relativi rispettivamente ad un servizio dati e fonia, TIM effettuerà la criptazione dei dati relativi ai recapiti telefonici del cliente finale (cfr. Allegato 3)

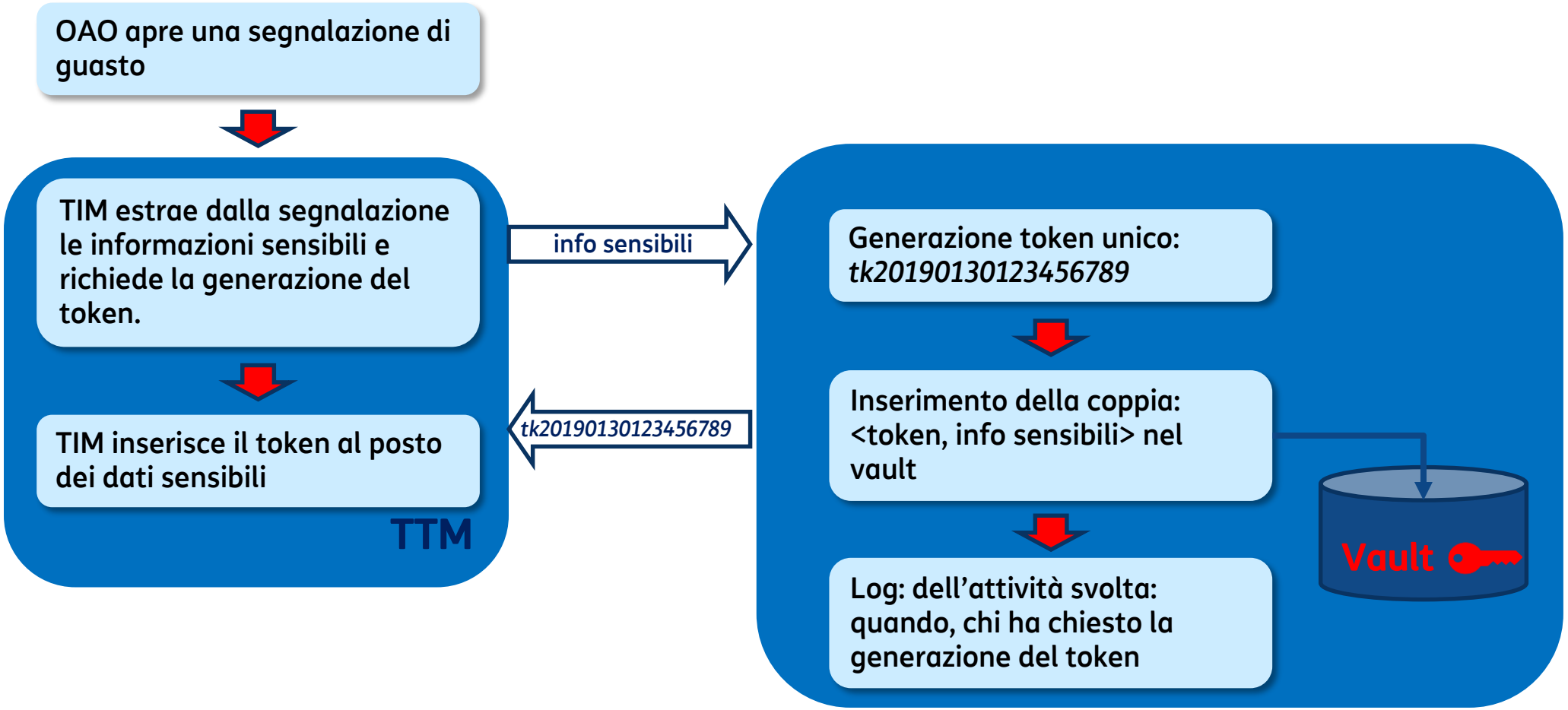
Fasi di progetto (1/4)

La criptazione delle informazioni sensibili per il processo di assurance, verrà sviluppata da TIM a valle della relativa condivisione da parte del Tavolo Tecnico e di AGCom

I **tempi di rilascio** in esercizio della soluzione informatica, saranno valutati da TIM a valle del consolidamento e dell'approvazione della soluzione di criptazione delle informazioni sensibili, descritta nel presente documento. Tali tempi saranno comunicati entro un mese dalla data di approvazione. Per quanto riguarda lo sviluppo dei log i tempi saranno comunicati a valle di approfondimenti giuslavoristici.

Le modifiche ai TR saranno pubblicate sul portale wholesale con almeno 90gg di anticipo rispetto al rilascio in esercizio

Fasi di progetto: Generazione del token e relativa gestione (2/4)



Fasi di progetto: Gestione operativa del token nella fase di avvio (3/4)

Tecnici On Field

I dati dell'anagrafica e quelli dei recapiti del cliente **sono trasmessi in chiaro** al momento della assegnazione della lavorazione della segnalazione:

- sullo smartphone del tecnico TIM;
- sul sistema di assegnazione dell'Impresa

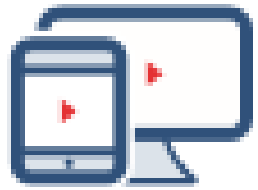
Il tecnico chiama il cliente con anagrafica e recapiti in chiaro.

Tecnici Back Office

I dati dell'anagrafica e quelli dei recapiti del cliente sono acquisiti dalla barra telefonica del tecnico di Back office al momento della lavorazione

Il tecnico al momento della lavorazione visualizza in chiaro l'anagrafica del cliente **ma NON i relativi recapiti**

Il tecnico può contattare il cliente utilizzando uno dei due recapiti telefonici che **non sono in chiaro** attraverso l'intermediazione della piattaforma Telefonica (CTI)



Per le strutture di back office che non utilizzano la barra telefonica verrà implementata una web-app.
il tecnico autorizzato all'accesso alla web-app:

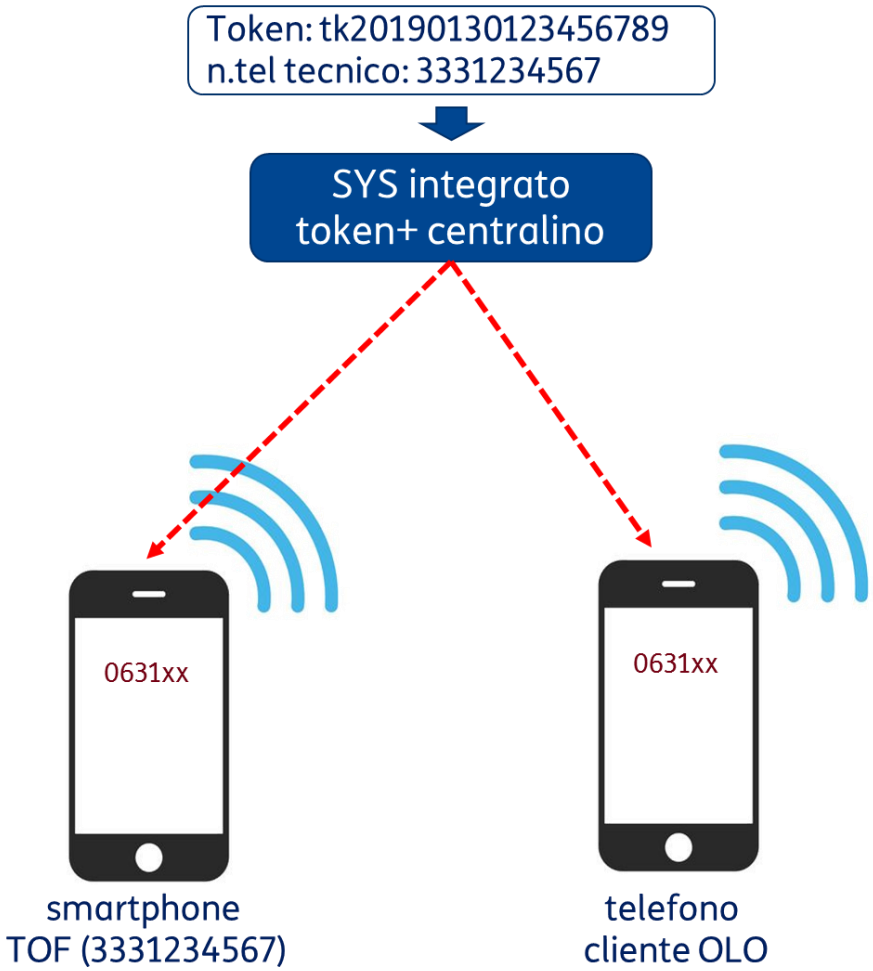
- inserirà il token
- otterrà in chiaro l'anagrafica cliente ed i due recapiti telefonici

Fasi di progetto: Gestione operativa del token nella fase a regime (4/4)

Al momento della assegnazione della lavorazione, sullo smartphone del tecnico **TIM NON saranno trasmessi in chiaro i recapiti telefonici**, sarà trasmessa in chiara l'anagrafica
Al momento dell'assegnazione della lavorazione (WR), sul sistema di assegnazione dell'Impresa, **NON saranno trasmessi in chiaro i recapiti telefonici** è sarà trasmessa in chiara l'anagrafica;

Il tecnico richiede al Sistema integrato di chiamare uno dei due recapiti tokenizzati

Il centralino mette in comunicazione il tecnico con il cliente senza visualizzare alcun numero chiamante



Per le strutture di **back office che NON hanno barra telefonica** verrà implementata una web-app:

- Il tecnico autorizzato all'accesso alla web-app, inserirà il token e otterrà in chiaro solo l'anagrafica cliente
- Il sistema integrato token+ centralino chiamerà sia il tecnico che il cliente mettendoli in comunicazione
- **Il tecnico non visualizzerà alcun numero chiamante** pertanto nel log delle chiamate effettuate sullo smartphone del tecnico on field, non resterà alcuna traccia del recapito telefonico del cliente

Allegato 1: Tracciato Record (1/3)

Il documento di TR pubblicato da TIM sul portale Wholesale in data 24 aprile u.s.:

- si applica per il WebService, ovvero per il colloquio B2B
- vale per le segnalazioni di Disservizio, Degrado o Richiesta di Supporto per i seguenti servizi:
  - BITSTREAM ASIMMETRICO ATM, BITSTREAM ASIMMETRICO GbE
  - Easy IP ADSL
  - BITSTREAM, VULA e Easy IP FTTH
  - BITSTREAM, VULA e Easy IP FTTC
  - ULL, ULL+NP, ULLD, ULLD+NP, SLU, SLU+NP
  - Shared Access
  - WLR, VULL

Per i servizi Wholesale non elencati nel punto precedente, la segnalazione di malfunzionamento da parte OAO può avvenire solo via GUI online mediante accesso da portale Wholesale.

Allegato 1: Tracciato Record (2/3)

Servizi dati: Bitstream Asimmetrico Atm e Gbe, Easy Ip Adsl, Easy IP NGA, Bitstream NGA, VULA

Nella tabella sottostante si riporta un estratto del tracciato record in esercizio (cfr pubblicazione del 20 aprile 2018) che elenca i campi di interesse ai fini della **criptazione/sovrascrittura** oggetto del presente documento.

Nome Campo	Descrizione del dato	Servizio		Xpath
		Formato	Dominio	
ANAGRAFICA_CLIENTE	Estremi del cliente finale, inteso come persona fisica o società Se non fornito in input, recuperato sul TT dalla banca dati TI	OPZ. Stringa (minLen 1)		/sm:createDataServiceRequest/sm:CustomerAccount/cst:Customer/cst:name
N_RECAP_CLIENTE	Recapito telefonico del cliente finale da contattare in caso di intervento on-field/altro	OBBL. Stringa Numerica (minLen 1) (maxLen 12)		/sm:createDataServiceRequest/sm:CustomerAccount/cst:Customer/cst:ConnectivityCFS/cst:NumericAddress/cst:number
N_RECAP_CLIENTE_ALT	Recapito telefonico alternativo del cliente finale da contattare in caso di intervento on-field/altro.	OPZ. Stringa Numerica (minLen 1) (maxLen 14)		/sm:createDataServiceRequest/sm:CustomerAccount/cst:Customer/cst:ConnectivityCFS/cst:NumericAddress/cst:NumericAddress/cst:number
NOTE_DISP	Note di disponibilità	OPZ. Stringa (minLen 1)		/sm:createDataServiceRequest/sm:CustomerAccount/cst:Customer/cst:notes
DIAGNOSI		OPZ. Stringa (minLen 1)	1 = Non si allinea modem ADSL 2 = Cadute Connessione ADSL 3 = Mancata Navigazione con Modem Allineato 4 = Navigazione Lenta Non previsto/ammesso per ID_TT: 110, 111, 112, 113, 114, 115 Obbligatotio per gli altri ID_TT	/sm:createDataServiceRequest/sm:TroubleTicket/cst:diagnosis

Allegato 1: Tracciato Record (3/3)

Servizi fonia: ULL, ULL+NP, ULLD, ULLD+NP, SLU, SLU+NP , Shared Access, WLR, VULL

Nella tabella sottostante si riporta un estratto del tracciato record in esercizio (cfr file pubblicazione del 20 aprile 2018) che elenca i campi di interesse ai fini della **criptazione/sovrascrittura** oggetto del presente documento.

Nome Campo	Descrizione del dato	Formato	Xpath
COGNOME_NOME / RAGIONE SOCIALE	Estremi del cliente finale, inteso come persona fisica o società. Se non fornito in input, recuperato sul TT dalla banca dati TI	OPZ. Stringa (minLen 1)	/sm:createUnbundlingServiceRequest/sm:CustomerAccount/cst:Customer/cst:name
N_RECAP_CLIENTE	Recapito telefonico del cliente finale da contattare in caso di intervento on-field/altro	OBBL. Stringa Numerica (minLen 1) (maxLen 12)	/sm:createUnbundlingServiceRequest/sm:CustomerAccount/cst:Customer/cst:ConnectivityCFS/cst:NumericAddress/cst:number
DIAGNOSI_OLO	Diagnosi effettuata Help Desk OLO/ISP. Campo a testo libero.	OBBL. Stringa (minLen 1)	/sm:createUnbundlingServiceRequest/sm:TelcoOperator/cst:TroubleTicket/cst:diagnosis

A questi campi verrà aggiunto il campo N_RECAP_CLIENTE_ALT

Nome Campo	Descrizione del dato	Formato	Xpath
N_RECAP_CLIENTE	Recapito telefonico del cliente finale da contattare in caso di intervento on-field/altro	OBBL. Stringa Numerica (minLen 1) (maxLen 12) Popolato con il recapito alternativodel cliente finale se ritenuto necessario dall'OAO oppure con «0» in alternativa	/sm:createDataServiceRequest/sm:CustomerAccount/cst:Customer/cst:ConnectivityCFS/cst:NumericAddress/cst:number

Allegato 2: GUI (1/2)

Servizi fonia: ULL, ULL+NP, ULLD, ULLD+NP, SLU, SLU+NP , Shared Access, WLR, VULL

Nella figura sotto riportata è cerchiato in rosso il campo di interesse della GUI ai fini della **sovrascrittura** oggetto del presente documento.

Allegato 2: GUI (2/2)

Servizi dati: Bitstream Asimmetrico Atm e Gbe, Easy Ip Adsl, Easy IP NGA, Bitstream NGA, VULA

Nella figura sotto riportata è cerchiato in rosso il campo di interesse della GUI ai fini della **sovrascrittura** oggetto del presente documento.

Allegato 3: Tracciato Record (1/3)

Nella tabella sottostante si riporta un estratto del tracciato record in esercizio (cfr pubblicazione del 20 aprile 2018) che elenca i campi in cui TIM continuerà a riportare le informazioni relative al cliente finale recuperata dal personale TIM in fase di lavorazione della segnalazione. Ci si riferisce al tracciato record **«Suspend»** usato da TIM per comunicare agli OAO la sospensione della lavorazione su un TT

Nome Campo	Descrizione del dato	Service		
		Formato	Dominio	Xpath
REFERENTE	Referente OLO/Cliente Finale con cui TI ha concordato l'appuntamento	OPZ. Stringa (minLen 1)		/sm:suspendRequest/sm:CustomerAccount/cst:name

Allegato 3: Tracciato Record (2/3)

Nella tabella sottostante si riporta un estratto del tracciato record in esercizio (cfr pubblicazione del 20 aprile 2018) che elenca i campi di interesse ai fini della **criptazione** oggetto del presente documento. Ci si riferisce al tracciato record **«setTestingFailureDataService»** utilizzata dall'OAO per comunicare a TIM l'esito negativo del collaudo da lui effettuato sul Trouble Ticket dichiarato risolto da TIM relativo ad un servizio dati

Nome Campo	Descrizione del dato	Service		
		Formato	Dominio	Xpath
N_RECAP_CLIENTE	Recapito telefonico del cliente finale da contattare in caso di intervento on-field/altro	OBBL.		/sm:setTestingFailureDataServiceRequest/sm:CustomerAccount/cst:Customer/cst:ConnectivityCFS/cst:NumericAddress/cst:number
N_RECAP_CLIENTE_ALT	Recapito telefonico alternativo del cliente finale da contattare in caso di intervento on-field/altro. Previsto ed ammesso per ID_TT = 110, 111, 112, 112, 114, 115. Non previsto/ammesso per gli altri ID_TT Campo Stringa che accetta solo caratteri numerici.	OPZ.		/sm:setTestingFailureDataServiceRequest/sm:CustomerAccount/cst:Customer/cst:ConnectivityCFS/cst:NumericAddress/cst:NumericAddress/cst:number

Allegato 3: Tracciato Record (3/3)

Nella tabella sottostante si riporta un estratto del tracciato record in esercizio (cfr pubblicazione del 20 aprile 2018) che elenca i campi di interesse ai fini della **criptazione** oggetto del presente documento. Ci si riferisce al tracciato record «**setTestingFailureUnbundlingService»** utilizzata dall'OAO per comunicare a TIM l'esito negativo del collaudo da lui effettuato sul Trouble Ticket dichiarato risolto da TIM relativo ad un servizio fonia.

Nome Campo	Descrizione del dato	Service		
		Formato	Dominio	Xpath
N_RECAP_CLIENTE	Recapito telefonico del cliente finale da contattare in caso di intervento on-field/altro	OBBL: Stringa numerica (minLen 1) (maxLen 12)		/sm:setTestingFailureUnbundlingServiceRequest/sm:CustomerAccount/cst:Customer/cst:ConnectivityCFS/cst:WirelineConnectivityCFS/cst:NumericAddress/cst:number