



NRTRDE - Near Real Time Roaming Data Exchange

Buyer's Guide

1 Introduction

Roaming fraud is a serious global concern for mobile operators. Nowadays combating and preventing losses caused by roamers' fraudulent behaviour represents a hot topic in mobile industry discussions. The GSMA community has worked out the best solution to combat roaming fraud: **NRTRDE** (Near Real Time Roaming Data Exchange). The implementation of the NRTRDE as mandatory system for all GSMA members shall be done by 1 October 2008. Operators may implement NRTRDE in advance of this deadline through bilateral agreements.

Operators and vendors have already started some preparations. Different implementation strategies, solutions and architectures have to be considered very carefully from several aspects.

Encapsulating several years experience in the roaming and fraud area Allround provides an overall insight of these new requirements. By collecting and answering the most typical questions that arise and going through the main responsibilities, this document¹ **aims to help operators to be prepared for the mandatory introduction of NRTRDE.**

2 Questions you will probably hear from your CIO

2.1 What is NRTRDE?

NRTRDE provides a more effective tool for operators to combat roaming fraud. This is a new method for reporting the customers' activities in the VPMN (Visited Public Mobile Network) networks and enables the HPMN (Home Public Mobile Network) to detect high network usage and other fraud issues in near-real time. Operators have to send limited, but enough information for fraud analysis while reducing the delay to less than 4 hours.

2.2 Why do we need to introduce it?

Aside from the fact that it will be **mandatory** there are several reasons for implementing NRTRDE:

- NRTRDE will prevent significant roaming fraud from occurring in the first place

¹ If you would like to use this material or a part of it please [contact us](#) and we can provide you with the power point version.



-
- Roaming partners will be pushing fraud loss liability onto VPMN. NRTRDE protects against the associated risks
 - Non-compliance of NRTRDE will badly affect roaming partnership

2.3 How should I approach NRTRDE?

However each operator is different, some typical behaviour can be observed:

- **Fingers-burnt:** Operators who already have had roaming fraud issues and revenue loss. They have a strong business case to introduce a roaming fraud solution.
- **Enthusiastic:** Operators who did not have issues but are conscious of the risk of roaming fraud and are willing to avoid it. They consider the mandatory implementation as an opportunity to get business advantage and implement real roaming fraud monitoring.
- **Reluctant:** Some operators will introduce NRTRDE only to comply with the requirements under the pressure of roaming partners, especially for sending NRTRDE files. They will not process the received NRTRDE records which have the risk to attract fraudsters. The consequences are the same as in case of risk-takers.
- **Risk-takers / Hazardous:** of course there will be operators who will ignore introducing NRTRDE, just recall the case of TAP3: several operators stayed for years at TAP2 version after the mandatory introduction of TAP3. But in this case the consequences are much harder: fraudsters are likely to move and target operators who do not implement NRTRDE. The global roaming fraud loss will be the same, but will be concentrated on a few operators.

2.4 How much would it cost?

According to preliminary estimations by GSMA member community introducing NRTRDE systems will cost approx. 350 k€ (100 k€ on sender side and 250 k€ on receiver side). The costs can considerably vary depending on the implementation model chosen, architecture applied and in some cases, the amount of records processed.

2.5 How to meet the 1 October 2008 deadline?

The NRTRDE is obligatory for every GSM operators. Of course there are some early-birds and late-implementers, but a big rush can be expected when most of the operators will start implementation to keep the deadline. If you want to have the best solution which perfectly suits your needs it is strongly recommended to start preparations in time. NRTRDE is a business and technical matter at the same time. On business level it is very useful to participate in [workshops](#) where you can share your ideas and learn experience from other operators. If you are interested in technical issues we recommend attending [training](#) organized in the subject.

2.6 Who will be involved from my organization? What kind of vendors to select and what criteria apply?

Although it brings many benefits introducing NRTRDE systems mean the biggest roaming change for operators since the introduction of TAP3. It is much more than a simple roaming data exchange: it affects both your internal processes and vendor relations. After completing several workshops with operators it is still not clear whether the main responsibility of NRTRDE belongs to roaming or fraud teams. However, it is clear that the departments and responsibilities listed below will be affected:

- Network management
- CDR collection
- Mediation
- Roaming management
- Fraud detection/management

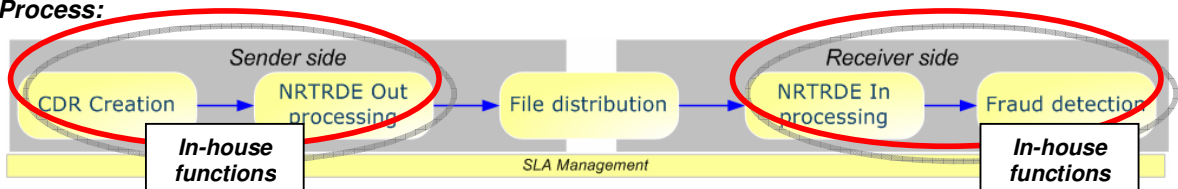


It seems that there is a typical misconception in NRTRDE which should be clarified: the DCH or the NRTRDE network providers will take over all responsibilities. Again, as in case of TAP, several functions can be done by the DCH and almost every operator has an in-house roaming management system but most DCH business is focussed on the transfer stage and not the entire process.

3 The NRTRDE process

Major steps	and	responsibilities:
CDR Creation management	sender side	switching/network
NRTRDE OUT Processing	sender side	roaming management
File Distribution/Exchange/Interchange	sender side	roaming management
NRTRDE IN Processing	receiver side	fraud management
Fraud detection	receiver side	fraud management
SLA management	sender/receiver side	

Process:



Architecture:



3.1 CDR Creation

Requirement: to have at disposal on the network side all CDRs that should be sent taking into consideration that the files have to be received by partner in 4 hours after the call has been completed

How to proceed?

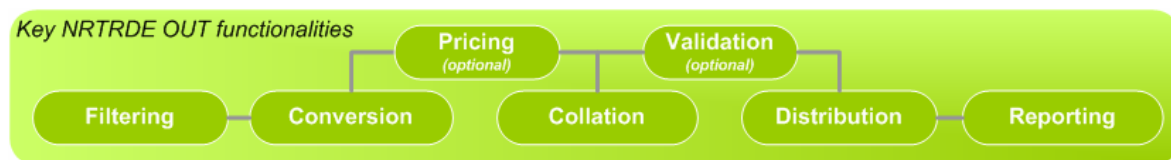
- Make an itemized inventory of all your network elements which creates the type of records specified in the relevant GSMA PRD FF.18
- Check whether all your network elements provide the records required
- Make sure that the collection process assures that the 4-hour requirement is met
- If not, contact your network equipment vendor and take actions

As you have probably realized already, the affected records are more or less the same as in case of TAP. Now, the most vital issue that can cause problems is the limited timeframe.

Some operators have foreseen that the network size (extended networks) might be a problem in record collection. In this case the solution is an adequate distributed architecture. If this applies to you too, [contact](#) us for more details.

Finally, one more advice: it is very important to make sure that the network management knows about this new requirement, respects it during the operation and takes into consideration each time when a new network element is introduced.

3.2 NRTRDE OUT Processing



Schematically, at the sender side the process can be split into two major parts: file creation and file transfer. While in the distribution phase operators have several options to decide, on the file creation phase, very similarly to the roaming (TAP) solutions, you have to set up the internal systems, processes and responsibilities.

Technical, business and legal aspects have to be taken into consideration to mark the borderline between tasks that should be done on your site and ones that are recommended to be outsourced to NRTRDE network providers. Similar to TAP file exchange there are several steps to do before your data is ready for distribution. You have to filter visitor records, convert and collate them before distribution – just to mention the most obvious tasks.

What you can achieve:

- Significantly reduced file conversion costs compared to DCH fees
- More flexible change management
- SLA proved – a guarantee in argued cases even with your distributor
- Flexible architectural solutions – supporting distributed architectures for extended networks
- Cost-effective communication within group members

With a good system implemented in-house you can be sure that you fully meet the NRTRDE requirements and keep the most vital parts of the process under your control. Besides you can significantly lessen costs - just consider you have to deal with at least 8-10 different file formats that have to be converted to a common format. Network service provider prices depend on complexity of the service – most slightly the license price does not depend on the volume of CDRs.



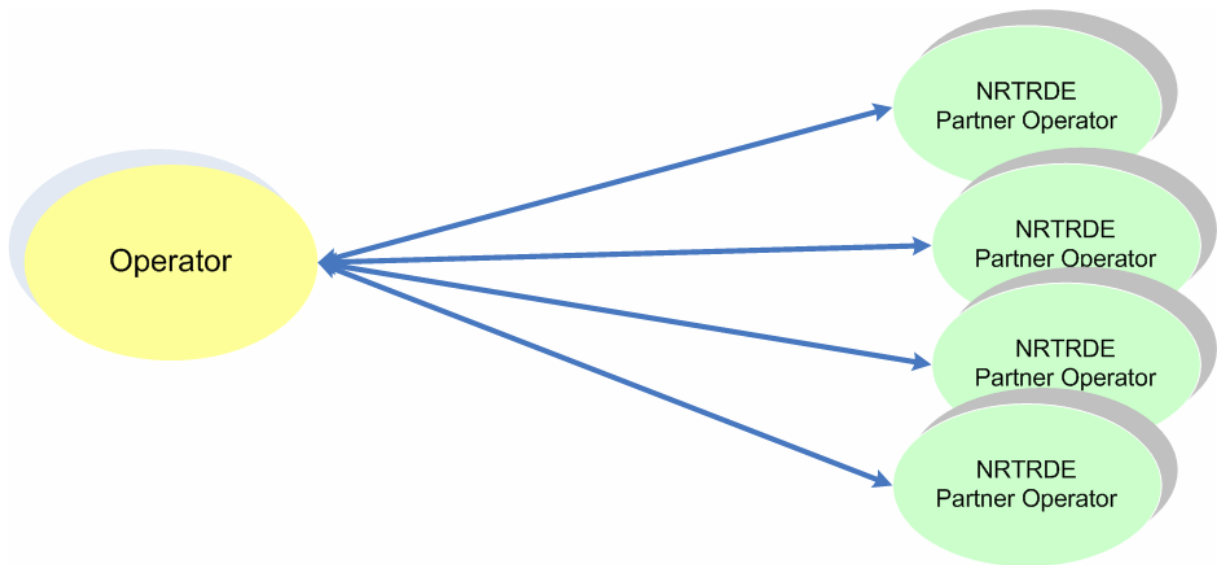
3.3 File Distribution / Interchange / Exchange / Transfer

Requirement: to send the valid NRTRDE files to your partners

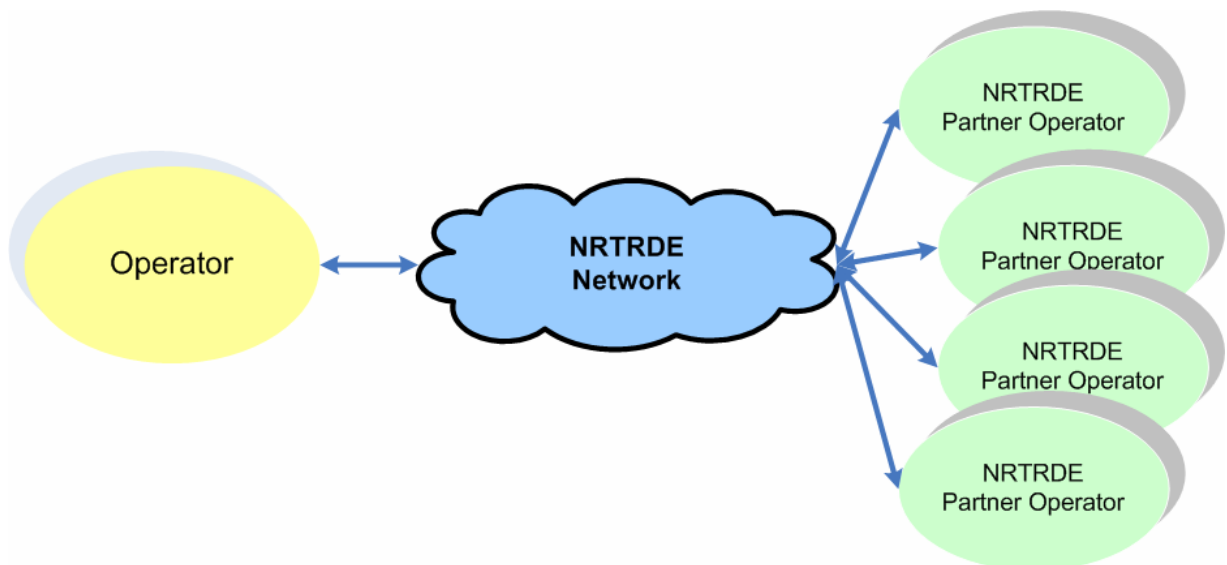
How to proceed?

You can distribute the NRTRDE files in two ways:

- directly with all your NRTRDE partners



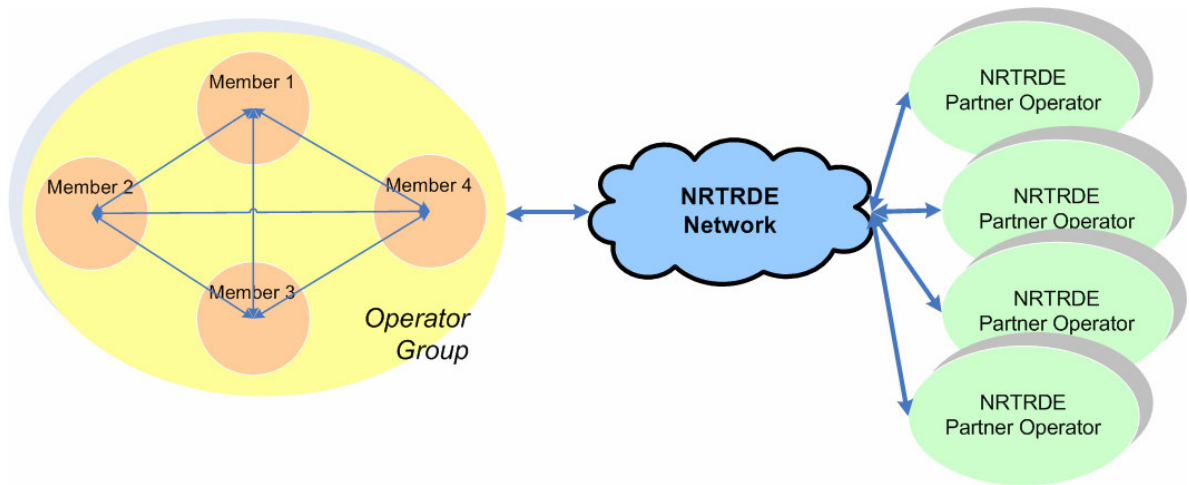
- using an NRTRDE network



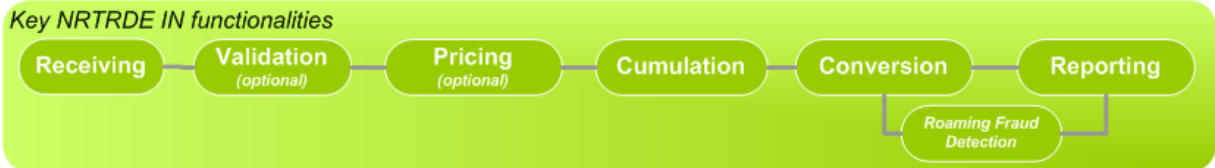


Direct connections can work but it requires such a cooperation which enables diagnostic and error handling properly. This is enormously resource and time consuming in case of a few hundred partners – be aware that sooner or later all your roaming partners will become NRTRDE partners as well! We recommend choosing file distribution services offered by your contracted data clearing house or call for services provided by the NRTRDE network providers (hubs) newly appeared on the market.

Extra tip: significantly lessen costs if operator groups optimize their file distribution actions by mixing the two solutions: direct distribution within the group and using an NRTRDE network for outside communication.



3.4 NRTRDE IN Processing



You need an NRTRDE system to receive the NRTRDE records, charge, convert and load them into the fraud management system. In order to effectively fight against roaming fraud your fraud detection system has to be able to evaluate the incoming data, monitor and take proper procedures to act. The border between the FMS and NRTRDE system is very flexible and should be optimized according to your needs and possibilities. If you do not have fraud detection system opt for a light-weight fraud detection solution. For further details see the [Fraud detection](#) chapter.

To protect your revenue you also have to operate an SLA functionality to continuously monitor and subsequently prove if your partners send you the files in time or not.

As in NRTRDE Out direction, also applies that significant cost reduction can be achieved by operating an in-house system.

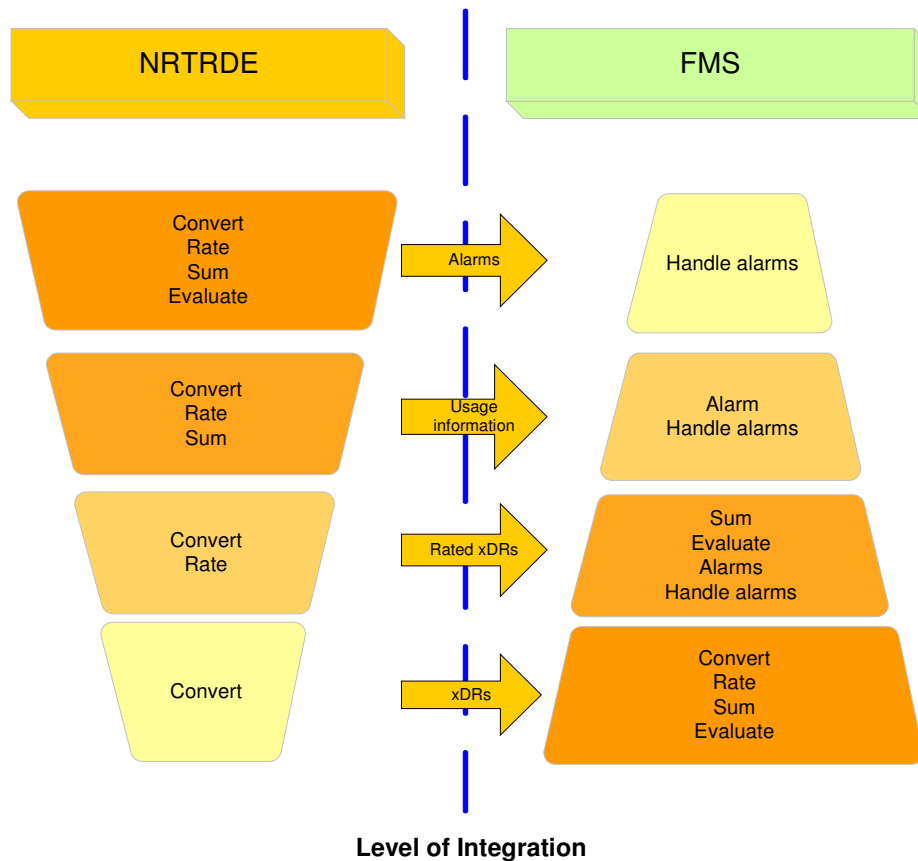


3.5 Fraud detection

One of the greatest advantages of NRTRDE is the reciprocity. If you send the NRTRDE files in time to your partner the HPMN takes the risk and responsibility for fraud detection. This is why is vital to build up a fraud detection system on receiver side. Let's see two different scenarios:

1. You already have a fraud management system

In this case the best choice is an integrated solution - you have to enable your FMS to handle NRTRDE. If it is feasible within the given deadline, go ahead! Contact your FMS vendor in order to extend the system with the new features required for handling NRTRDE. But if any issues occur that may affect the functionality, price or deadline it is recommended to set up the optimal balance by substituting the necessary functionalities missing from your FMS:



2. You do not have a fraud management system or cannot enable the existing one to handle NRTRDE

Evaluating the data sent by your NRTRDE partners and monitoring roaming fraud it is a must otherwise you risk that your network will be targeted by fraudsters and become a risk-taker. Since the deadline is close do not start now purchasing a new one or replacing the existing one. Choose a light-weight roaming fraud detection system which focuses squarely on roaming fraud. Allround offers such a complementary system which offers the necessary functionality but it does not intend to replace a full-featured FMS and maintains the upgrade possibility to full-featured FMS.



3.6 Service level management (SLA management)

However the goal of the NRTRDE is to minimize risk and clearly set up responsibilities there can occur disputed matters and conflict of interest. For this reason it is vital that parties should be able to prove their rights effectively and with optimal cost. If we say that the NRTRDE is the “third-party insurance”, the SLA management is the “Casco insurance” – if investing in the NRTRDE implementation is a must, investing in SLA management is a strongly recommended option to protect yourself.

The main problem is the lag time between the data exchange and the revenue loss caused by proven fraud. In this case the responsibility is on VPMN to prove several months after the fraud event that the information have had been sent to HPMN in time. A good SLA management functionality smoothly, cost efficiently and effectively provides the accurate information to protect you in two aspects:

- Continuously proves that you keep the 4 hour requirement
- Proves that your partner sends files late.



4 RealXS – your NRTRDE Solution

Allround realized the significance of the problem of roaming fraud and are prepared to offer NRTRDE solution in a modular way to best fit the operators' need and architecture. Answering the increasing need for high quality NRTRDE solutions we launched RealXS, a new generation NRTRDE solution. RealXS is a standalone system running at operators' site enabling them to be NRTRDE compliant both on sender and receiver side.

RealXS enables operators to manage and control the NRTRDE process and optimize the balance between:

- in-house and outsourced responsibilities
- CAPEX/OPEX

In the entire spectrum of possibilities RealXS offers an alternative and complementary solution at the same time to the available offers on the market.

Our RealXS solution is one-time license sales fee based and without any recurring and hidden costs.

In the entire spectrum of possibilities RealXS offers an alternative and complementary solution at the same time to the available offers on the market

Key solution differentiators:

- Scalable solution that works with both the NRTRDE service provider and in house Fraud/Roaming teams
- Eliminates the risk of outsourcing all Roaming Fraud to a 3rd party - the solution works with existing fraud applications
- Requires minimal resources to manage the application in house - bird's eye view
- Allround currently have 2 existing NRTRDE implementations with 2 leading European mobile operators
- Operators who are part of one telecom holding company can communicate directly (without the need for a NRTRDE service provider) whereas those operators who are individual entities can use NRTRDE service provider to distribute
- Improved file routing with Intelligent Routing which defines multiple routes, alarms and reports if one fails
- Proven ROI within 1 year
- Comprehensive training incorporated with the installation

5 About Allround

With a presence in 4 continents - North-America, Europe, Middle-East, Africa – and more than 20 countries Allround pioneered commercial CDR/xDR processing and is a leader in roaming solutions and the billing testing area.

ALLROUND puts telecom operators in control with applications for Billing System Testing, CDR/xDR Handling and Analysis, TAP Conversion, Roaming Management, Fraud Detection, and Revenue Management. We achieved a unique and niche position in the market as industry specialists as

- **key supplier of roaming management systems** with more than 13 new operator implementations worldwide in the last 18 months
- winner of the **World Billing Awards 2006** in Best Revenue Assurance / Management Project Category
- the first **testing tool - CeDaR - attested by BABT** (British Approvals Board for Telecommunications) against its Code of Practice for the design and supply of communication support system



ALLROUND is an ISO 9001:2000 certified, profitable, private European company with a global customer base. The company is an Associate Member of GSM Association since April 2002.

Allround is a strong supporter of the NRTRDE in its product line since the first version has been introduced. Allround developed both a standalone solution and an integrated one into its Fraud Detection System and carried out two successful implementation projects at T-Mobile Hungary and T-Mobile Slovakia.

Allround is involved in relevant GSMA groups: NRTRDE Steering Committee, BARG, TADIG:

- It guarantees that Allround's solutions are fully compliant with the current and future GSMA specifications (such as BA.20, FF.18, TD.35).
- Allround hosted the TADIG#59 (May 2005) and TADIG#63 (May 2007)
- Facilitated a separate, one-day workshop with experts from up to 20 operators to discuss key issues of implementing NRTRDE.

For more information contact:

Gábor Lakatos

Director, Marketing and Sales

E-mail: lakatosg@allround.eu

www.allround.eu