GIA et sécurité des applications

Bruno Guay

Symposium GIA 2017

2017-03-01

nurun
services conseils

Plan

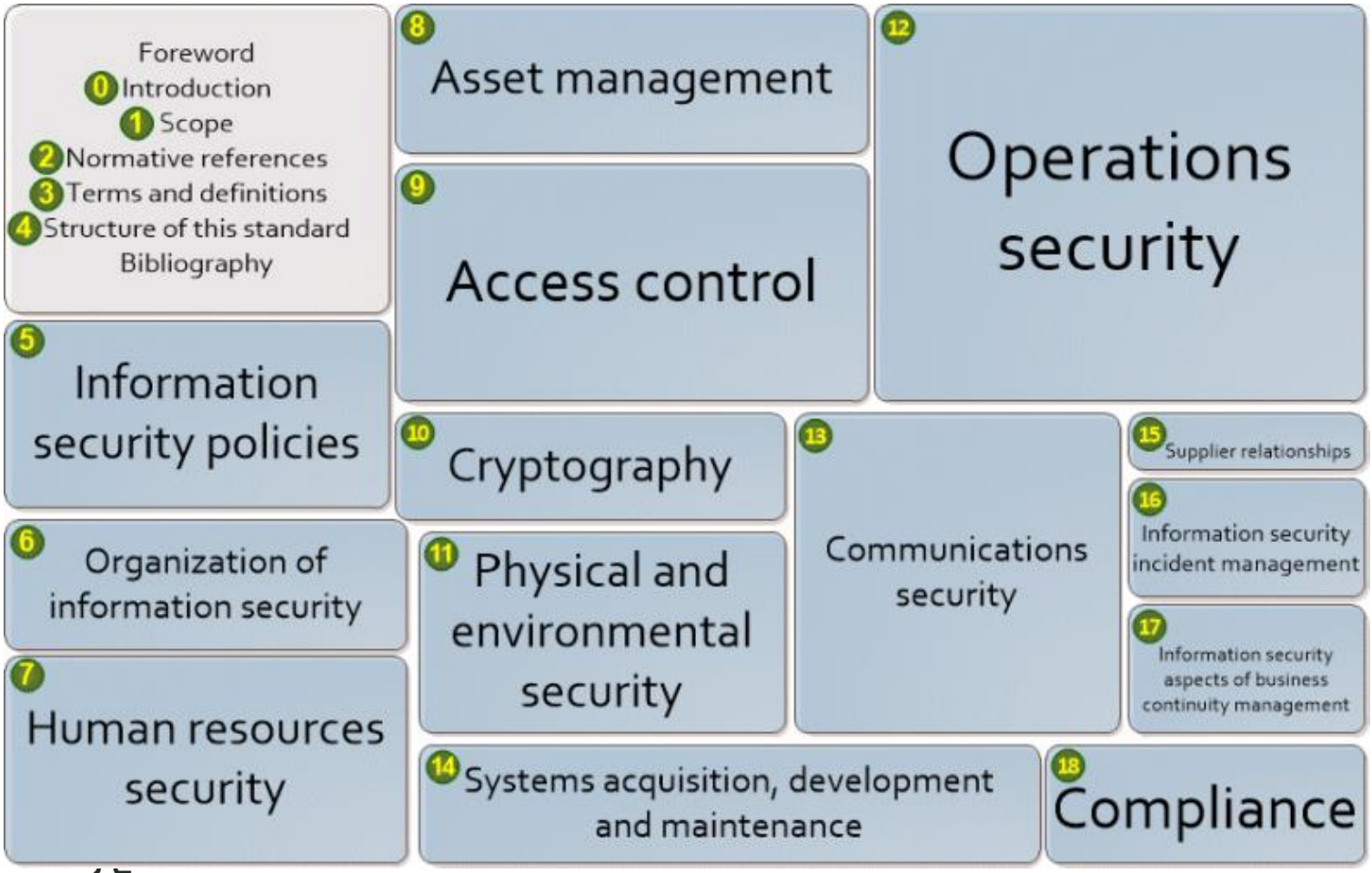
- Contrôle d’accès et GIA
- RBAC
- ABAC
- Web Access Managers
- Fédération d’identités
- Applications en Infonuagique
- IAM as a Service

nurun
services conseils

CONTRÔLE D'ACCÈS ET GIA

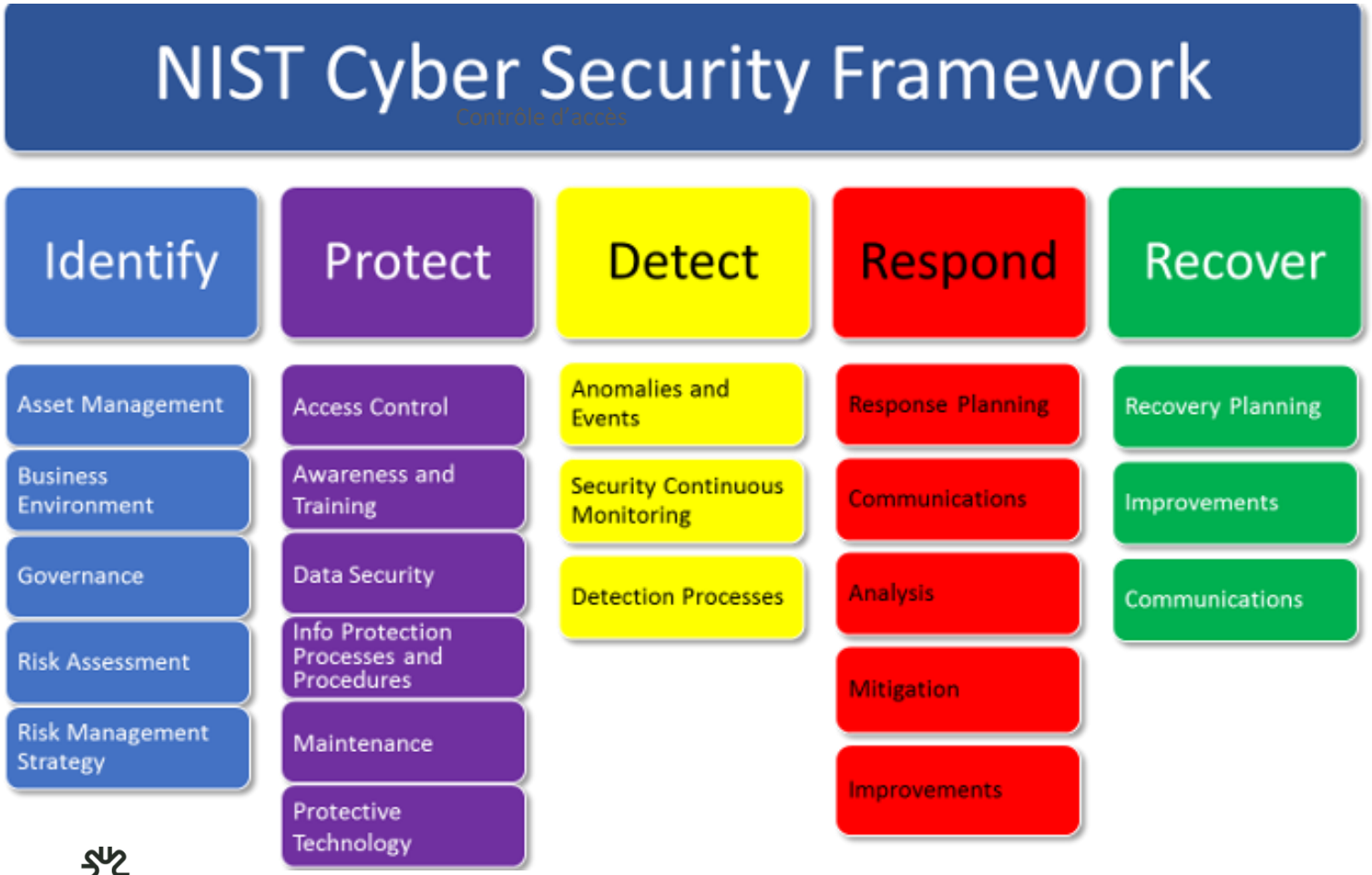
nurun
services conseils

Contrôle d'accès selon ISO 27002



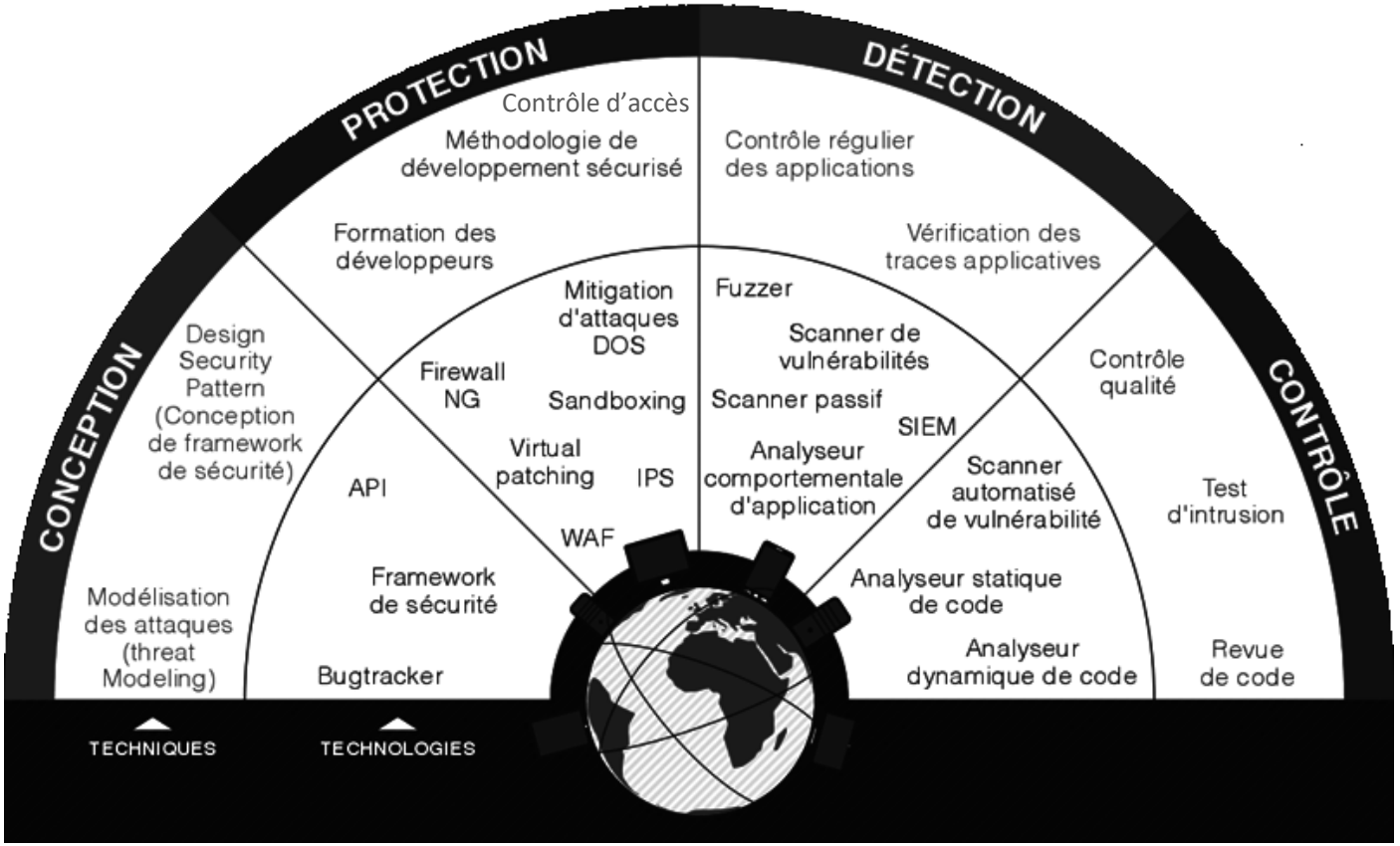
nurun
services conseils

Contrôle d'accès selon NIST



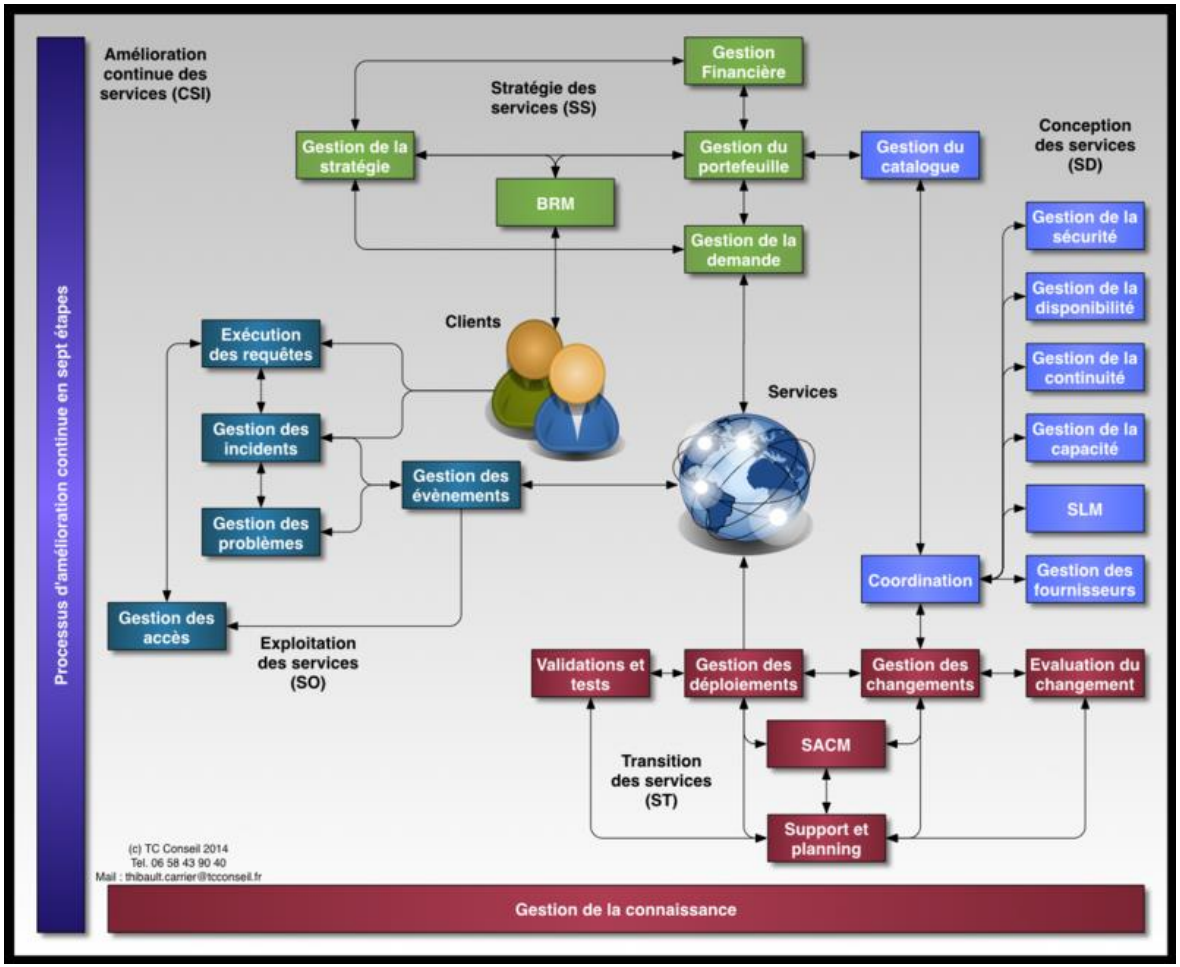
nurun
services conseils

Contrôle d'accès parmi les contrôles applicatifs



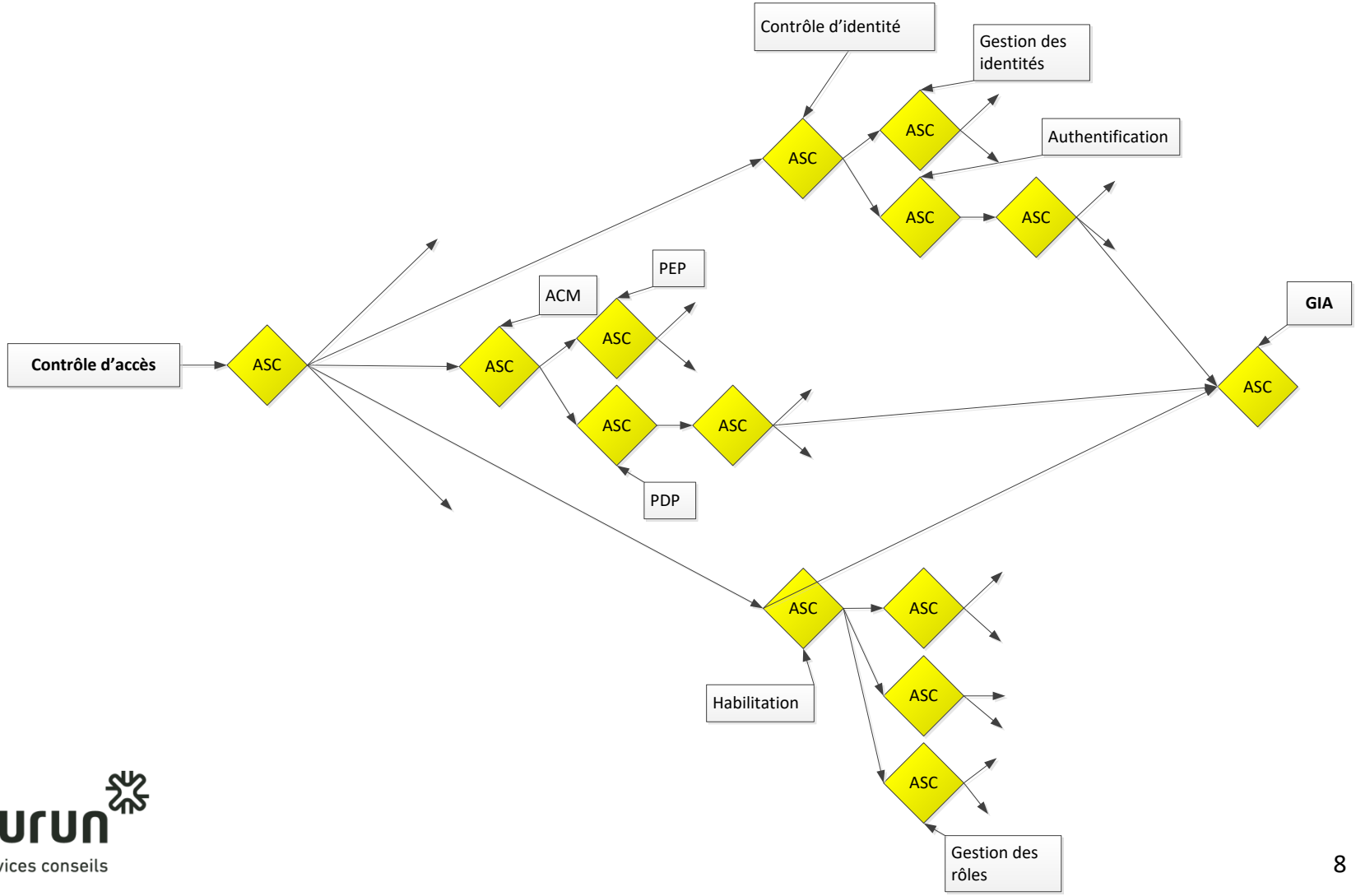
Source : advens.fr

GIA selon ITIL



nurun
services conseils

Contrôle d’accès selon ISO 27034

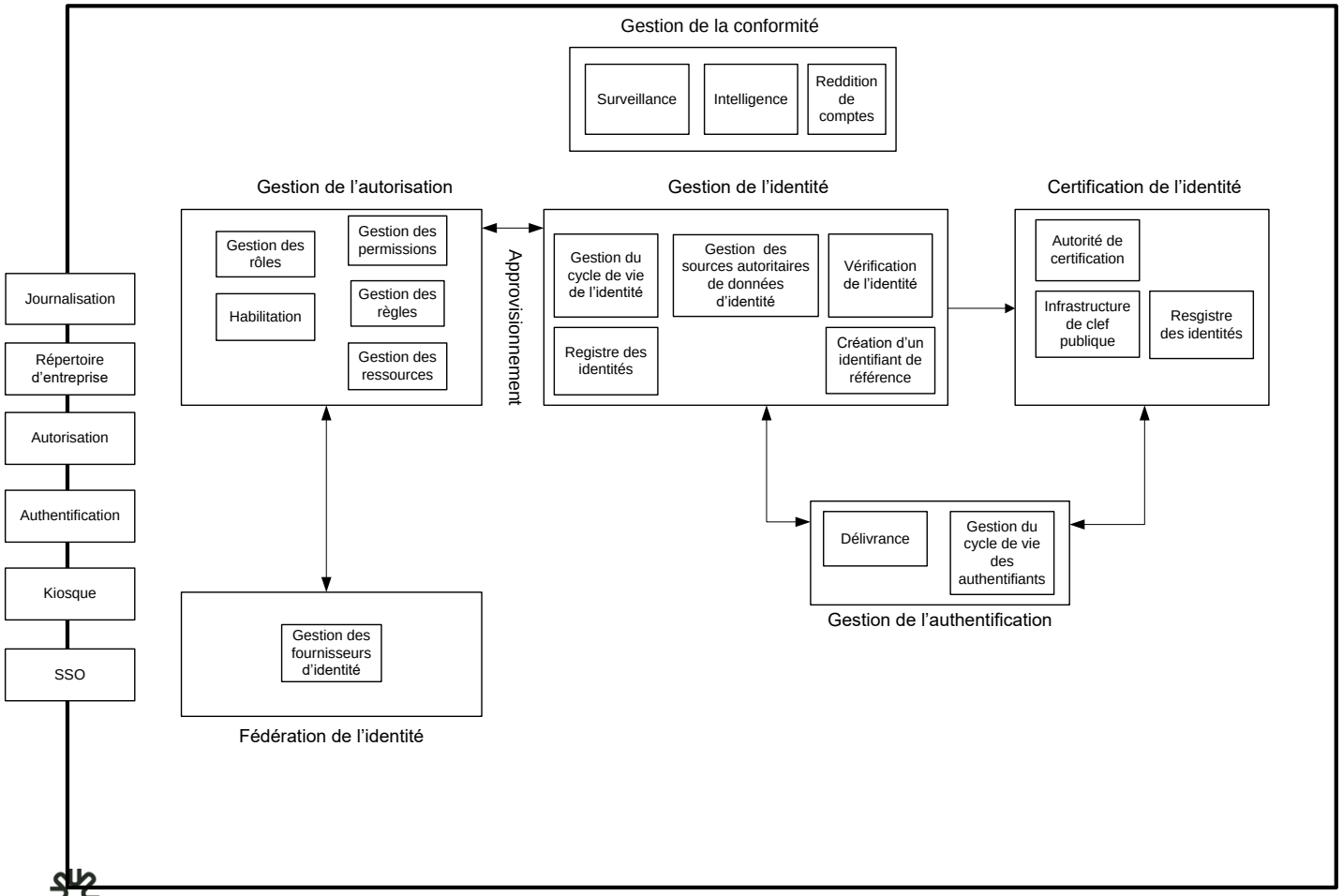


nurun
services conseils

Services de GIA

- La GIA est un ensemble de processus et de techniques qui améliorent l'efficacité et l'efficience du contrôle d'accès.
- Une solution de GIA peut être décrite en une architecture de services internes et externes à la solution
  - qui encapsulent les processus et les techniques
- Certains de ces services sont disponibles pour les applications.

Services de la solution de GIA



RBAC

nurun
services conseils

Modèle RBAC de base

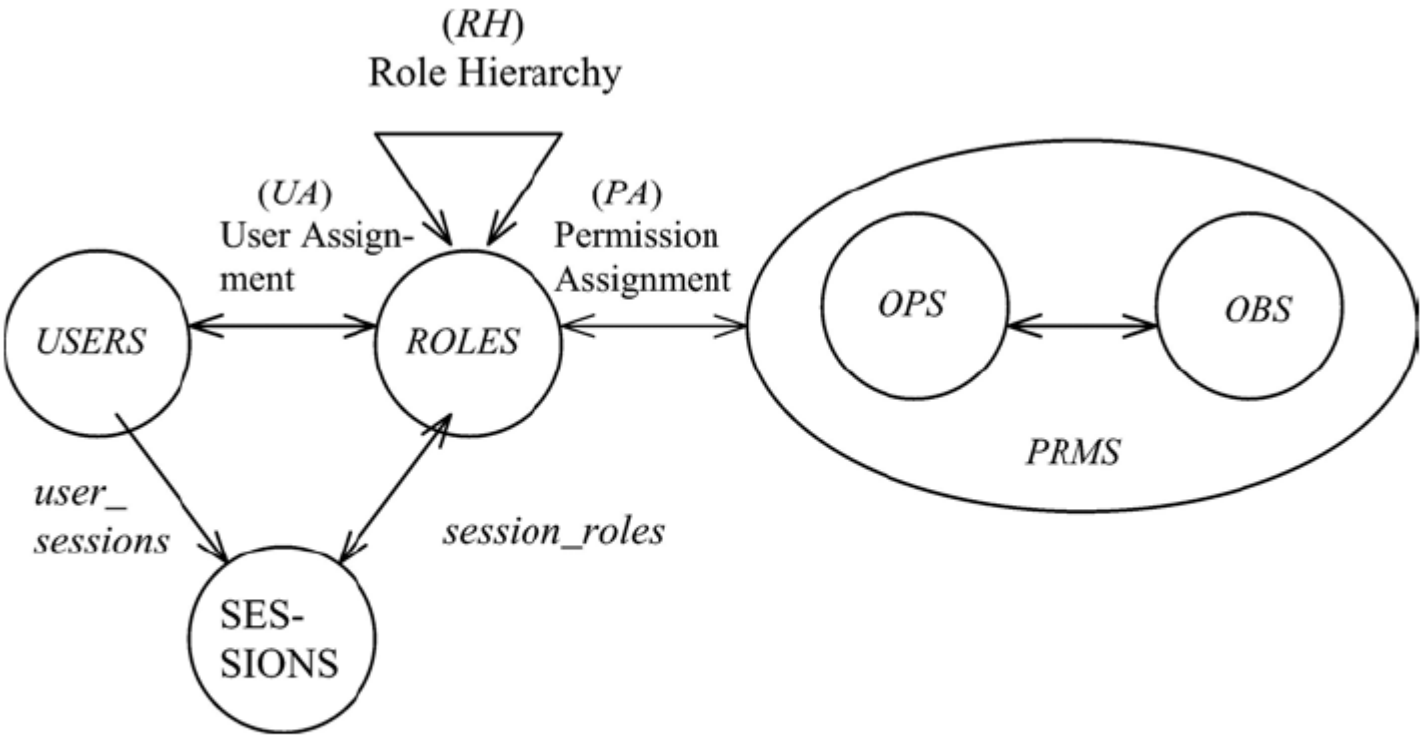
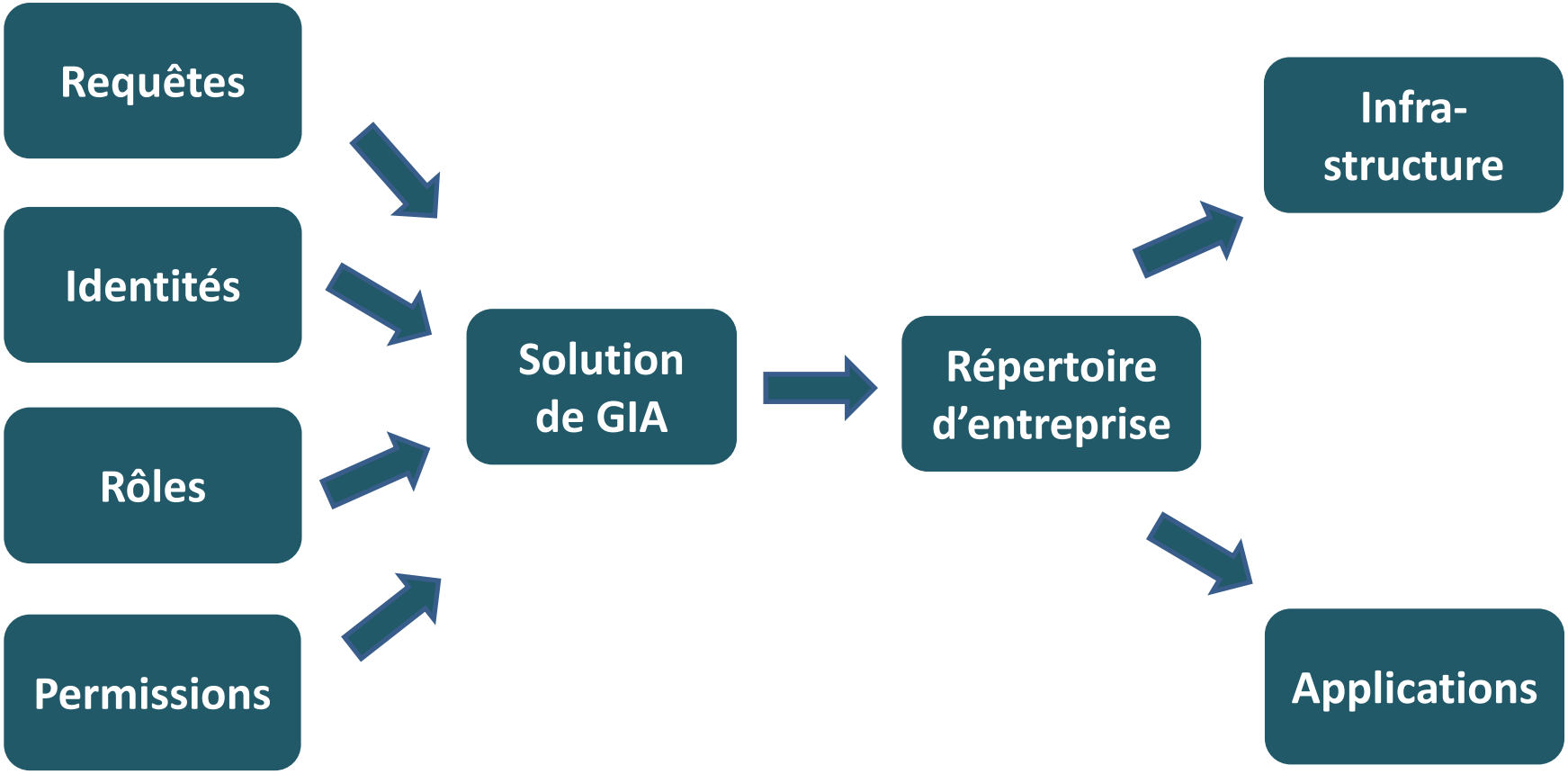


Figure 2: Hierarchical RBAC

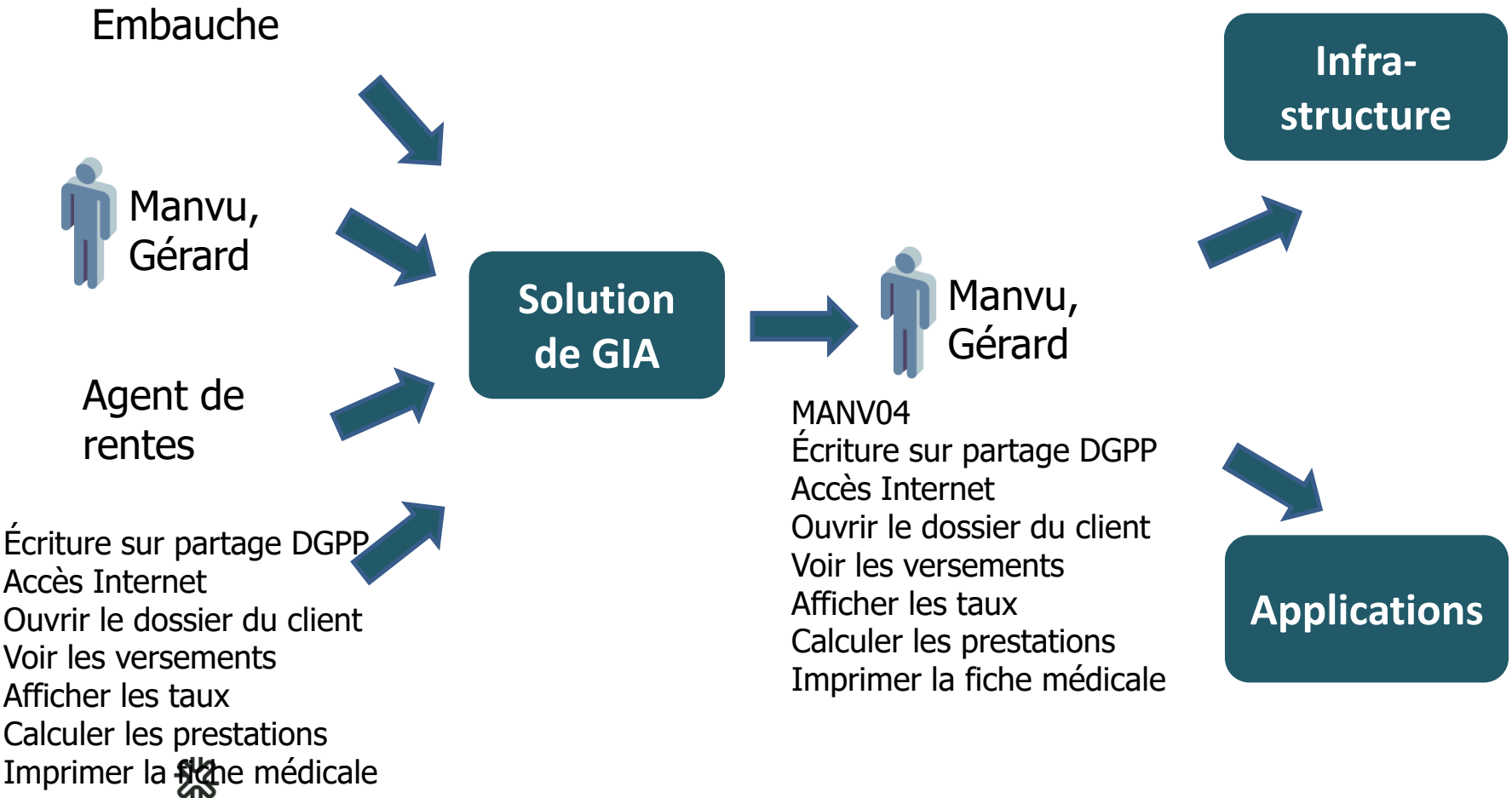
nurun
services conseils

Solution standard



nurun
services conseils

Solution standard



nurun
services conseils

Limites RBAC

- RBAC n’est pas adapté aux situations où un contrôle granulaire des accès est nécessaire
- La gestion des accès s’effectue sur deux niveaux ou portées, souvent selon des modèles et des processus différents:
  - le niveau d'entreprise, qui propose des rôles organisationnels et de métier, ainsi que des permissions sur des actifs d'entreprise et sur l'infrastructure; et
  - le niveau applicatif, qui propose des rôles ou des permissions dont la portée est limitée à une seule application.

Limites RBAC

- La cause de cette dualité est le facteur de **coût de gestion** des accès.
- L'avantage économique du modèle RBAC est qu'il permet de diminuer le coût de l'habilitation, en assignant des regroupements de permissions prédéfinis (des rôles) à des regroupements d'individus.

Limites RBAC

- Cette économie dépasse le coût de gestion des rôles tant que les conditions suivantes sont vraies:
  - tous les individus d'un regroupement accomplissent les mêmes tâches qui nécessitent les mêmes permissions;
  - les permissions nécessaires à l'accomplissement de ces tâches changent peu; et
  - il y a un nombre suffisant d'individus dans chaque regroupement.

Limites RBAC

- Dans le cas contraire on observe, en réponse aux besoins changeants de l'entreprise,
  - une dégradation de l'utilisation du modèle si les processus de GDA ne sont pas mis en force, ou
  - une explosion du nombre de rôles si les processus sont mis en force.
- Ces deux réactions entraînent une augmentation du coût de gestion des accès.

Limites RBAC

- On observe que les trois conditions sont plus facilement respectées pour la gestion des accès au niveau d'entreprise où le niveau de granularité est bas et les changements moins fréquents.
- Pour le niveau applicatif où le niveau de granularité des permissions est élevé et les changements sont plus fréquents, le modèle RBAC devient moins adéquat.
- Si on tente d'appliquer strictement le modèle RBAC pour l'autorisation applicative, les deux réactions mentionnées ci-dessus seront observées.
- On atteindra rapidement un point où l'augmentation du coût de gestion des rôles dépassera la diminution du coût de l'habilitation apportée par RBAC.
- En bref, RBAC n'est pas « rentable » à un niveau de granularité élevé.

Est-ce bien une limite de RBAC?

- L’erreur fréquente est de croire que les rôles ont nécessairement une portée organisationnelle.
- En fait le modèle RBAC n'a pas la notion de portée.
- On peut donc l'appliquer concurremment et différemment au niveau d'entreprise et au niveau applicatif.
- Note: RBAC a aussi la notion de hiérarchie de rôles
  - un rôle d’entreprise peut « contenir » un rôle applicatif
  - mais c’est peu utilisé.

RBAC à deux niveaux

- C'est un compromis acceptable car:
  - les compétences requises pour la modélisation des rôles applicatifs sont différentes de celles requises pour les rôles d'entreprise;
  - les compétences requises pour la gestion opérationnelle des accès applicatifs sont différentes de celles requises pour les accès d'entreprise;
  - les permissions applicatives sont souvent plus dynamiques et dépendantes d'un contexte d'affaires, par exemple elles sont souvent régies par le concept de dossiers ou cas courants;
  - les applications elles-mêmes sont en évolution constante;

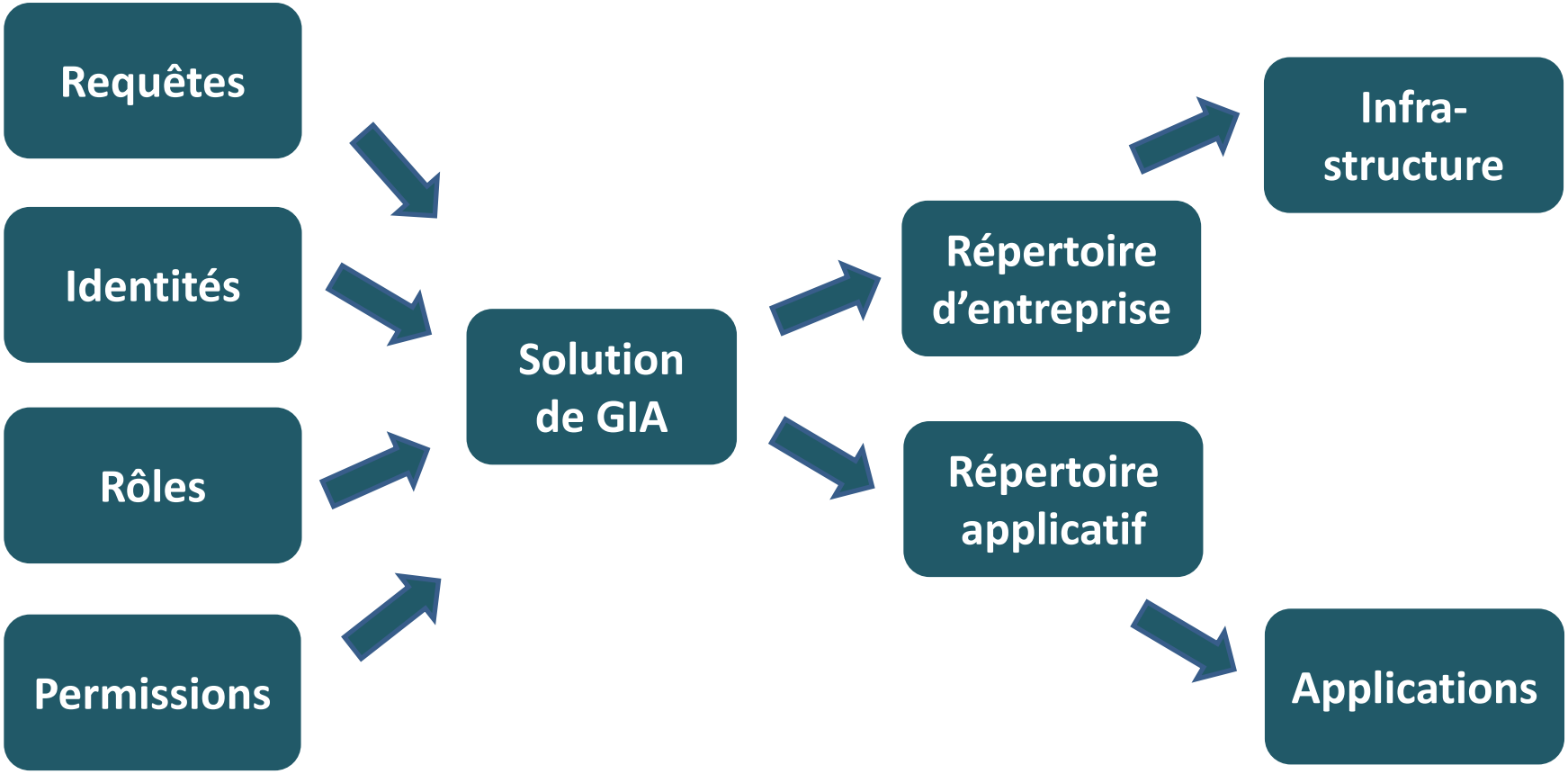
RBAC à deux niveaux

- les responsabilités sont différentes -- les détenteurs et les approbateurs sont généralement différents;
- les processus de gestion des accès applicatifs sont souvent différents, par exemple on voit souvent les dossiers courants être assignés par des chefs d'équipe ou des répartiteurs; et
- les permissions dans les applications sont inutilement détaillées pour les gestionnaires qui approuvent l'habilitation au niveau d'entreprise.

RBAC à deux niveaux

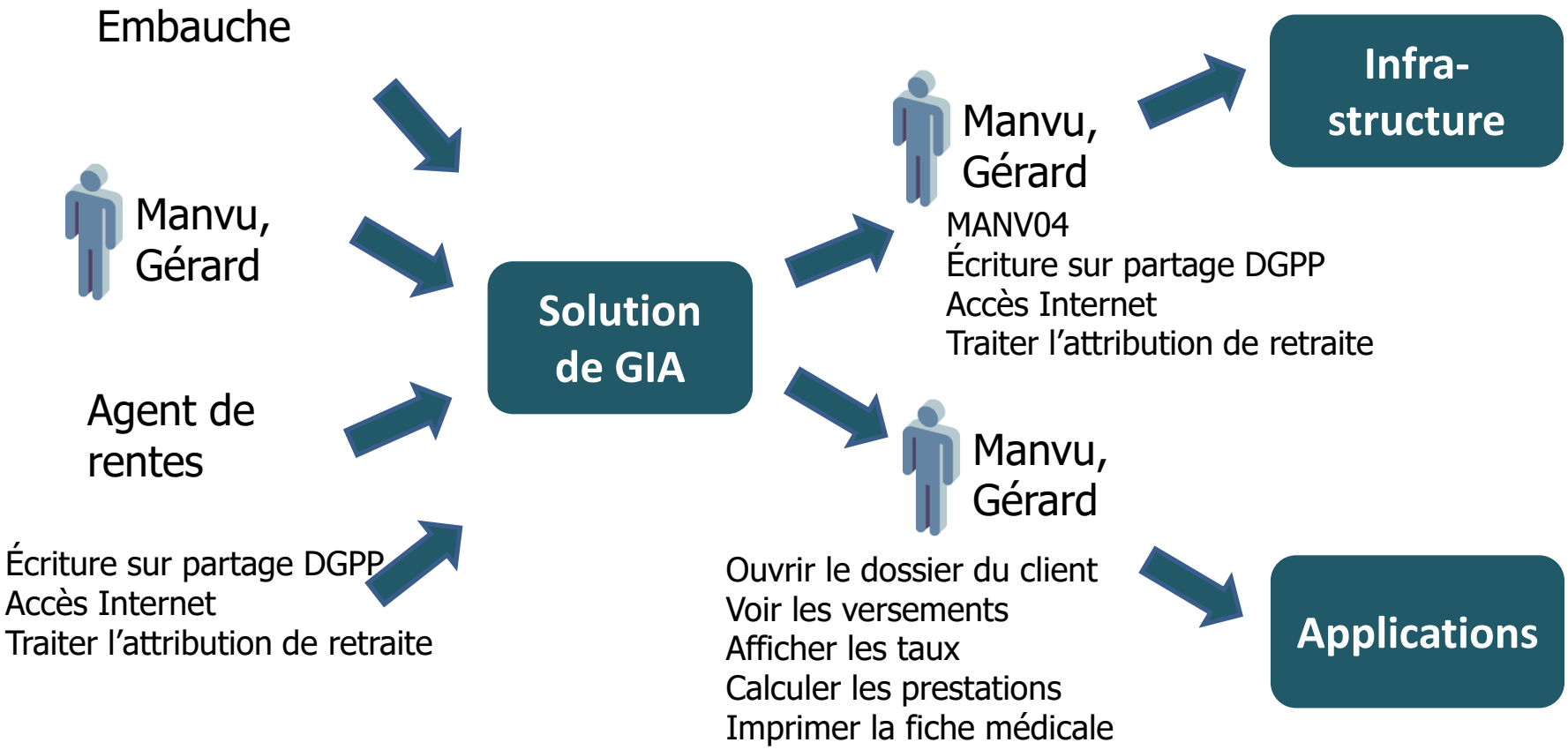
- Les permissions reliées aux rôles d'entreprise sont représentées dans le répertoire d'entreprise.
- Certaines permissions sont en fait des rôles applicatifs.
- Les rôles applicatifs sont détaillés en permissions applicatives dans le répertoire applicatif.
- Les permissions applicatives ne sont pas représentées dans le répertoire d'entreprise.

RBAC à deux niveaux



nurun
services conseils

RBAC à deux niveaux



nurun
services conseils

Raisons techniques

- Il y a aussi des raisons techniques et technologiques pour implémenter un répertoire applicatif distinct.
- Les répertoires d'entreprise sont optimisés pour l'authentification et non pour l'autorisation.
- Les répertoires d'entreprise sont utilisés pour gérer les domaines, les configurations et les politiques, ce qui limite la flexibilité
  - par exemple pour créer de multiples environnements: production, essais, développement
- En particulier avec Active Directory:
  - le schéma est peu extensible;
  - le jeton Kerberos est limité.
- Le répertoire applicatif peut répondre à différents protocoles standard: LDAP, SQL, services web
  - Des API sont disponibles pour les développeurs.

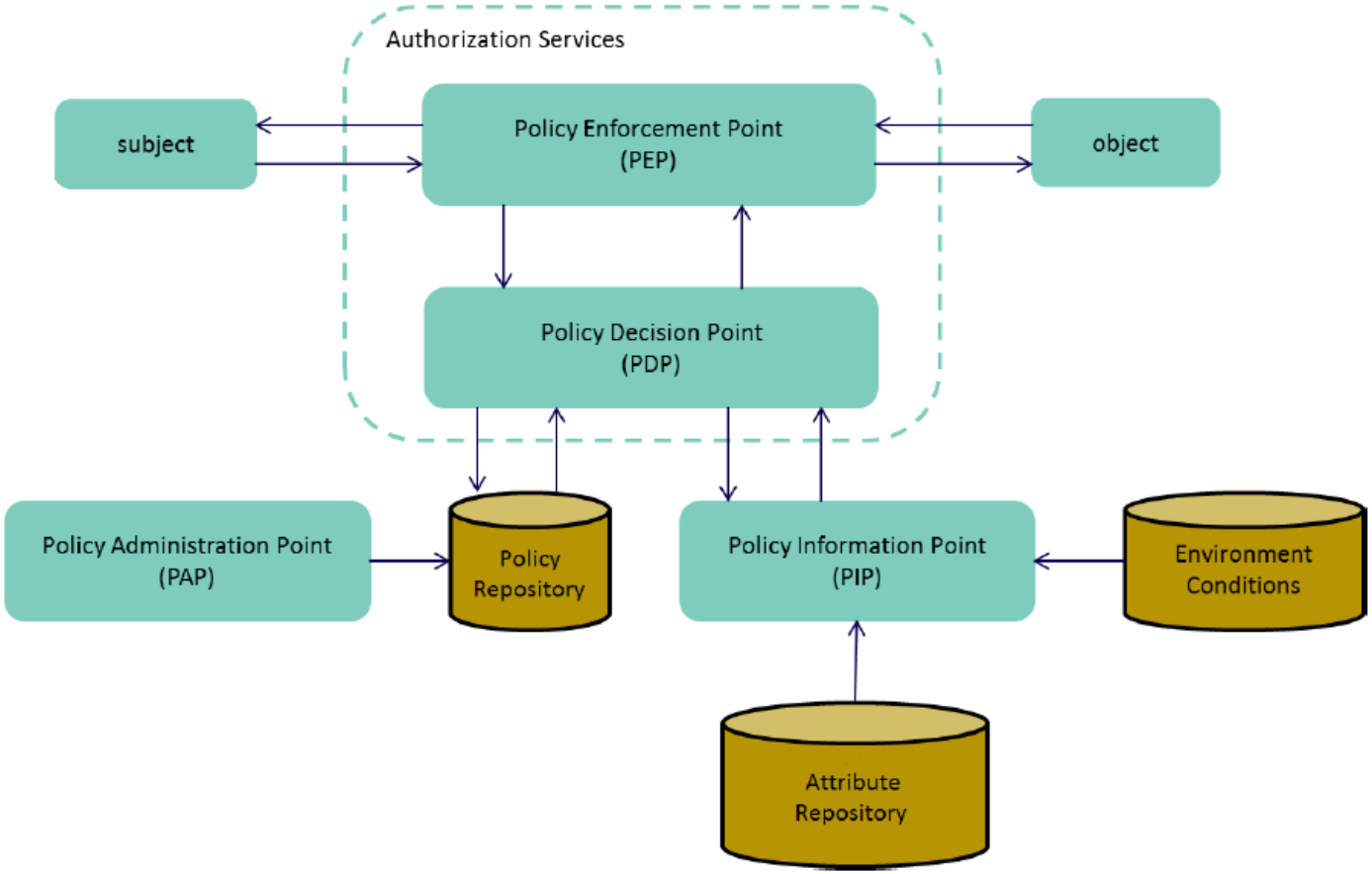
ABAC

nurun
services conseils

ABAC

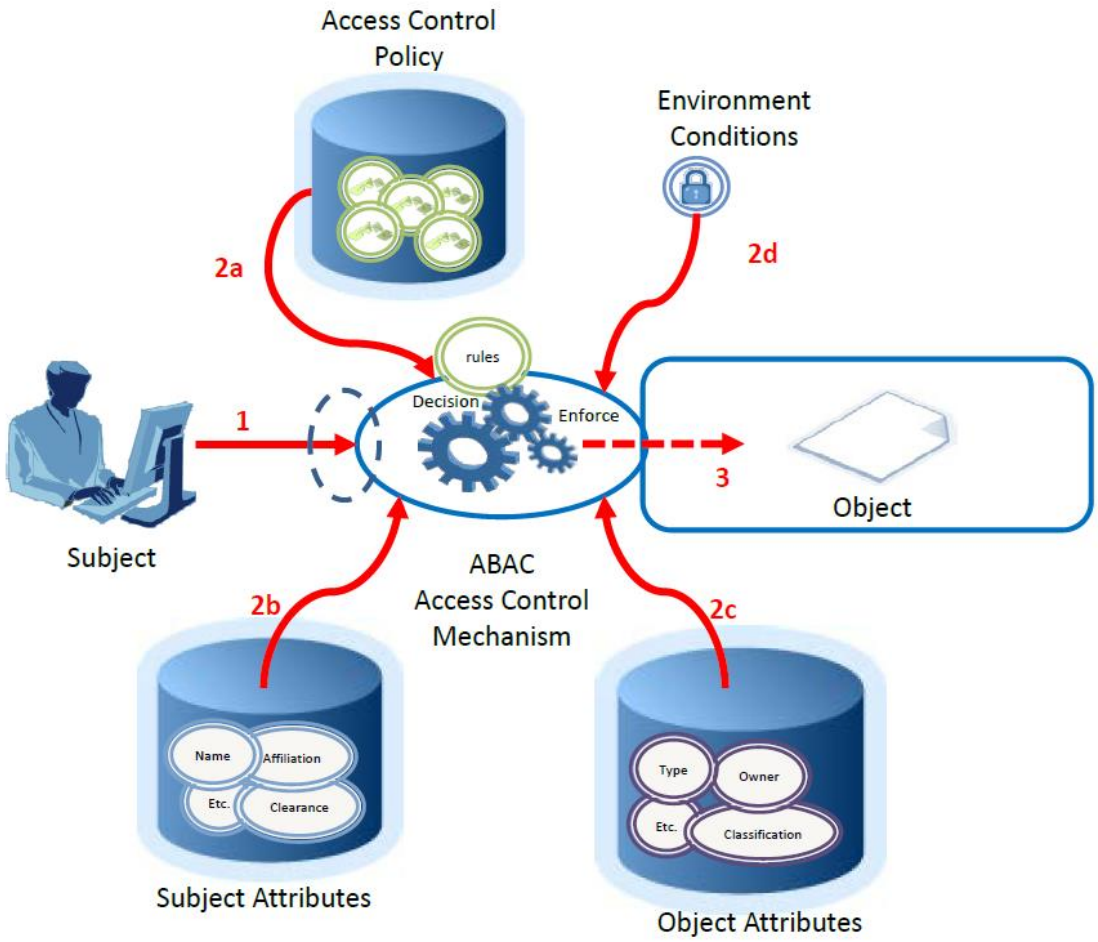
- RBAC-A, ABAC, PBAC, RAdAC et RB-RBAC apparentés.
- ABAC (Attribute-Based Access Control) est décrit par la norme NIST SP 800-162 (mêmes auteurs que RBAC).
- On peut voir ABAC comme une généralisation de RBAC
  - l'appartenance d'un sujet à un rôle est un attribut parmi d'autres.
- ABAC permet plus de flexibilité dans la prise de décision.

Composants ABAC



nurun
services conseils

Survol ABAC



nurun
services conseils

Caractéristiques ABAC

- Plus de flexibilité dans la prise de décision.
- Moins de travail pour établir des liens statiques entité-rôle et rôle-permission.
- Plus de travail au moment de la prise de décision (impact de performance).
- Meilleur contrôle d'accès en conditions changeantes.
- Plus difficile de retracer la justification d'une décision prise à un moment précis
  - importance de la journalisation.
- Fortement recommandé de documenter les règles en langage d'affaires
  - et la raison de chaque règle
  - comme on documente du code.
- Plus difficile d'appliquer des politiques d'entreprise centralisées (PBAC).
- Il faut associer des attributs aux objets (métadonnées).
- La gestion des attributs peut être déléguée

Exemple ABAC 1

- Règle: tous les vendeurs ont accès en lecture aux soumissions envoyées aux clients dans leur région de vente.
- L'accès devrait être permis pour la requête suivante:
  - Attribut du sujet "department"="Ventes"
  - Attribut du sujet "sales region"="Estrie"
  - Action="read"
  - Attribut de l'objet "type"="Soumission"
  - Attribut de l'objet "region"="Estrie"
- Les attributs sont requis de sources autoritaires: système de GRH pour le département, CRM pour la region, GID pour le type de document.

nurun
services conseils

Exemple ABAC 2

- Règle: Un utilisateur dont le rôle est « Agent de rentes » et ayant réussi la formation « Attribution de retraite» peut voir et ouvrir la corbeille « Dossiers d'attribution de retraite » pendant les heures normales de bureau. Il peut voir dans la corbeille les dossiers dont l'attribut « Assignation prioritaire » a la valeur de son numéro d'employé.
- La formation est fournie par le système de gestion de talents.

Exemple ABAC 3

- Règle: Un utilisateur dont le rôle est « Médecin » ou « Infirmière » de type « Clinique » et ayant réussi la certification « Règles de PRP HIPAA » peut lire et ajouter des notes dans un dossier de type « Patient » du même « GMF » dont l'attribut « Consentement GMF » est « Oui ».

Exemple ABAC 4

- Règle: Un utilisateur dont le rôle est « Conseiller en architecture » affecté à un projet est collaborateur du site du projet (accès en écriture).
- affectation de l'utilisateur: code de projet autorisé dans le système de feuilles de temps
- Rôle de l'utilisateur: système de GRH

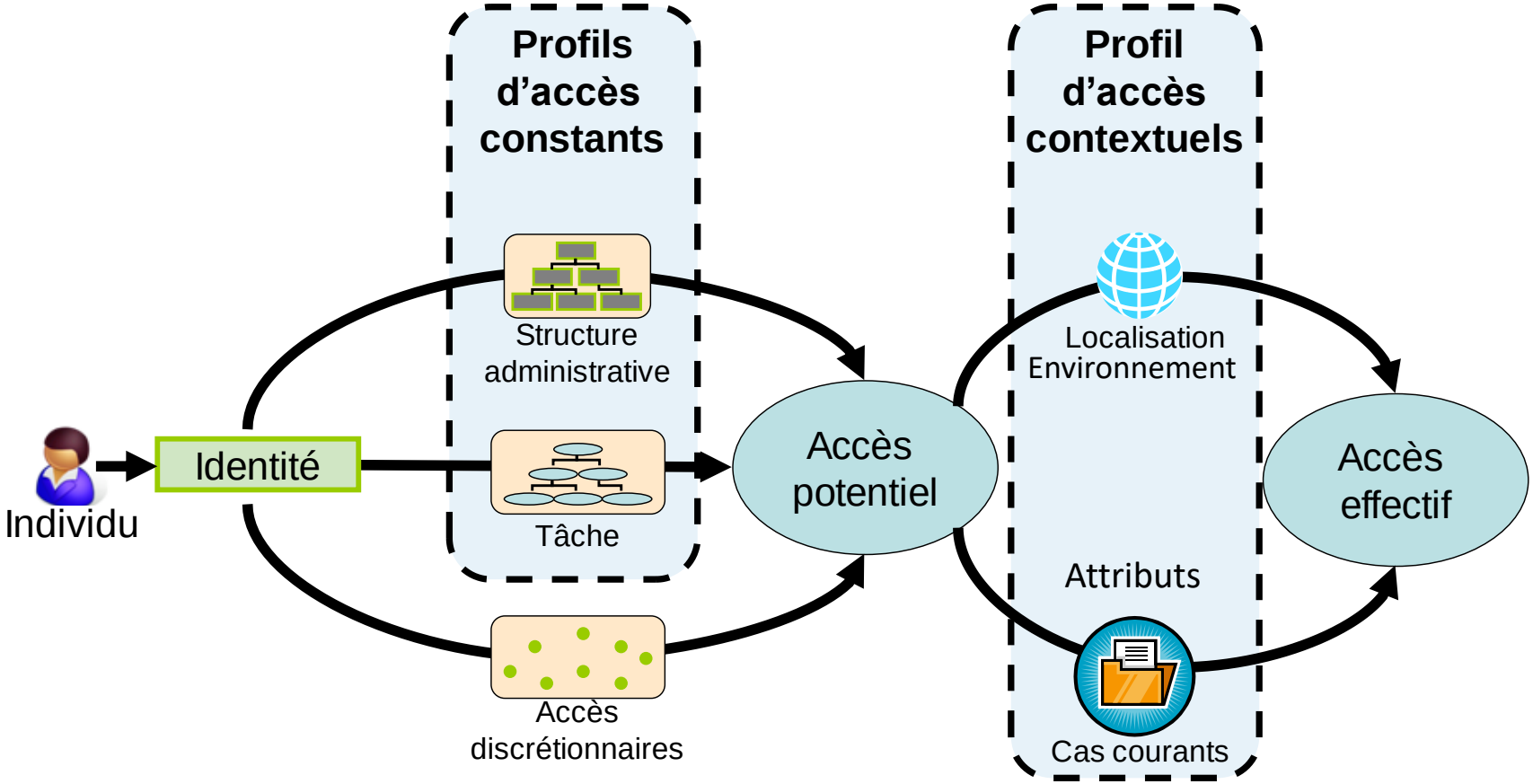
Constats ABAC

- Les caractéristiques de ABAC le rendent pertinent pour les applications, peu pour l'infrastructure.
- Quelques solutions commerciales ABAC pour applications, web services, BD.
- Surtout des Web Application Managers.
- Quelques modules spécialisés (ex: Berkeley ESSP pour SharePoint 2013).
- On a investi dans RBAC.
- On n'a pas terminé l'implantation de RBAC.

Solution réaliste?

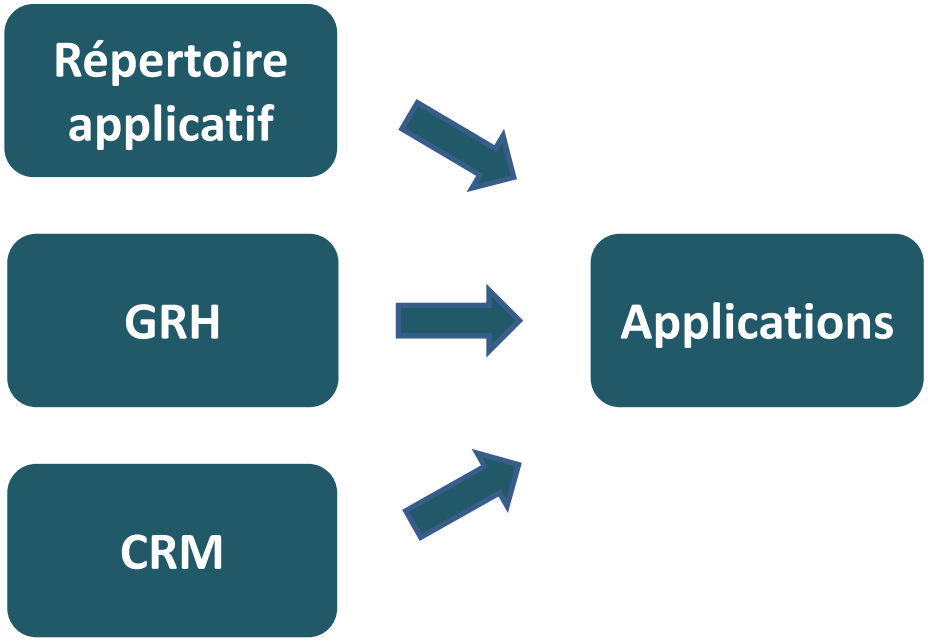
- L'erreur fréquente est de croire que le traitement des règles doit s'effectuer en un seul temps (un seul PDP) avec tous les attributs.
- En fait le modèle ABAC ne met pas de contrainte d'implantation.
- On peut imaginer un traitement ABAC en deux étapes:
  - rôles et permissions pour les accès potentiels, surtout à l'infrastructure;
  - autres attributs pour limiter ces accès de façon dynamique, surtout aux applications.
- On bâtit du ABAC par-dessus le RBAC.
- Le résultat final est presque le même.

Exemple d'un modèle réaliste



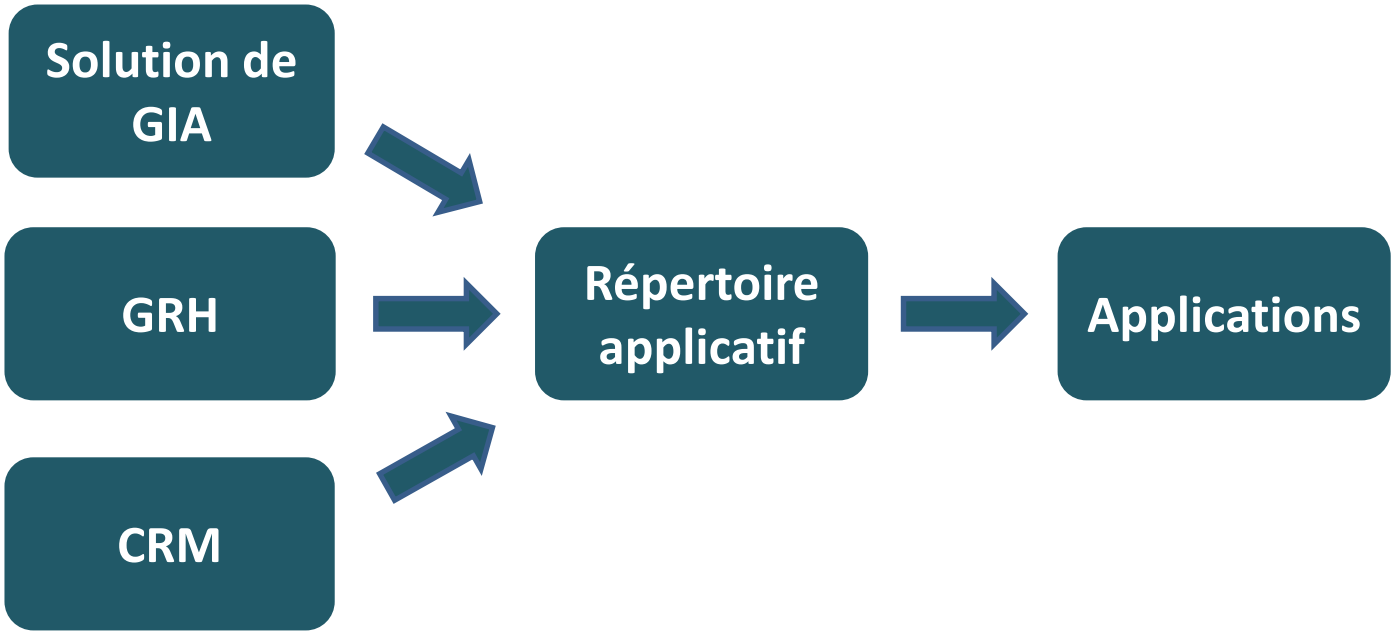
nurun
services conseils

Implantation ABAC 1



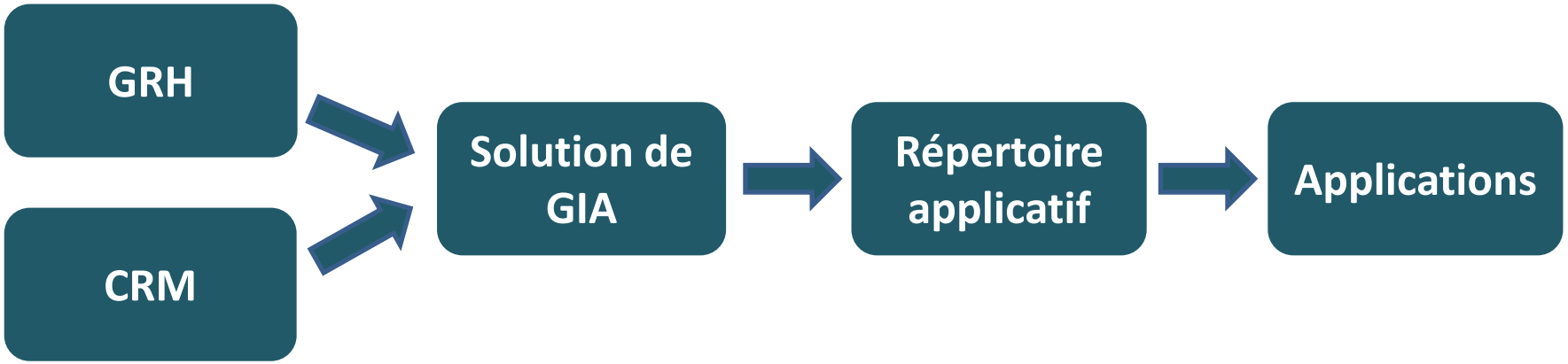
nurun
services conseils

Implantation ABAC 2



nurun
services conseils

Implantation ABAC 3



nurun
services conseils

La solution de GIA pour unifier le tout

- Permet la communication des attributs des sources autoritaires vers les PDP.
- Empêche la prolifération des traitements et des communications.
- Réduit l’impact sur les sources autoritaires.
- Permet un niveau élevé de confiance grâce à l'authentification forte, le chiffrement, et autres contrôles.
- Permet le partage et la conversion d'attributs entre systèmes et entre organisations.

nurun
services conseils

WEB ACCESS MANAGERS

nurun
services conseils

Survol WAM

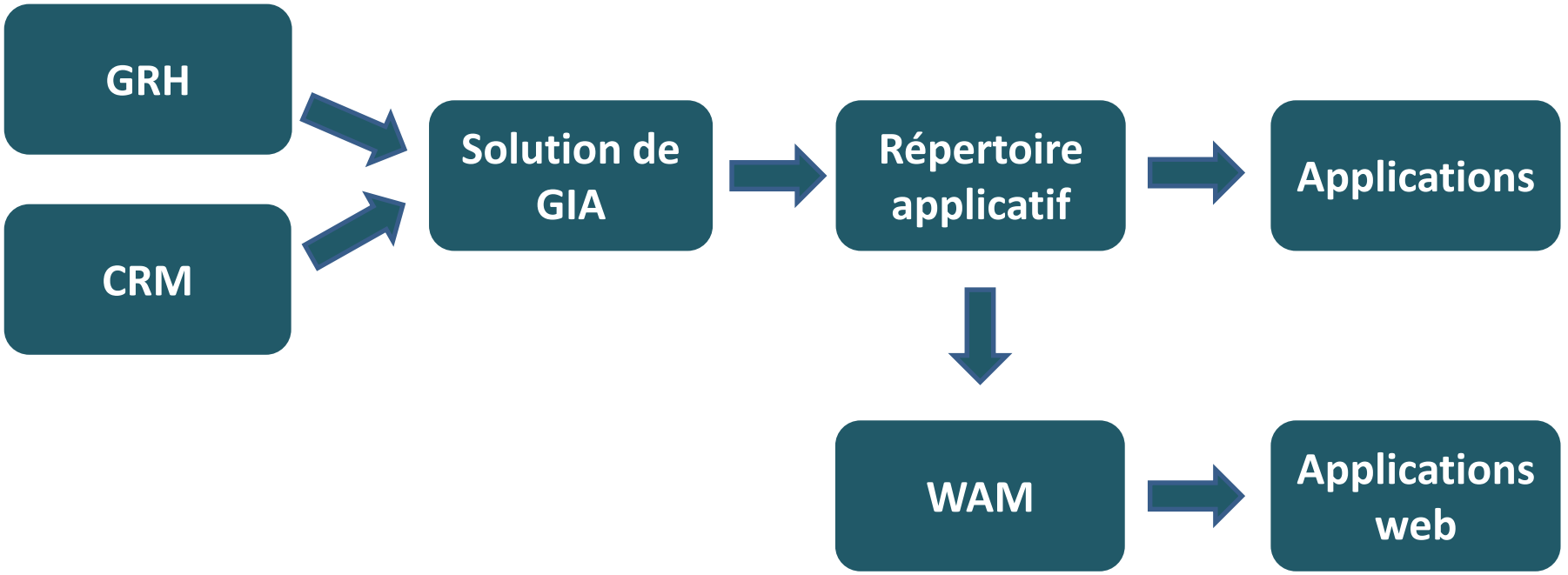
WAM ou Web SSO

- Une solution de contrôle d'accès aux applications web par les utilisateurs internes et externes
- Permet de sécuriser et moderniser les applications web existantes
  - par exemple celles qui n'exercent aucun contrôle d'accès applicative
  - par exemple celles qui ne journalisent pas les accès
  - avec impact minimal: peu ou pas de changements aux applications
  - en améliorant les interfaces, ex: écran d'authentification personnalisé

Fonctions WAM

- Contrôle d'accès
  - par page, basé sur rôles, attributs, environnement (ABAC)
  - Idéalement transparent, ex: filtre ISAPI, reverse proxy
- Authentification
  - avec niveau d'assurance basé sur le risque pour chaque page
  - nombreuses méthodes d’authentification forte
- Gestion du risque en continu
  - évaluation continue de la confiance en l'identité
  - détecte les changements inhabituels: emplacement, appareil, système, etc.
  - ex: banques
- SSO pour toutes les applications web de l’entreprise
- Injection de données
  - dans les en-têtes, les requêtes ou les réponses http
  - pas recommandé: nécessite des changements à l’application
- Balancement de charge et haute disponibilité
- Fédération d’identités: contrôleur d’accès et fournisseur d’identités

Implantation WAM



nurun
services conseils

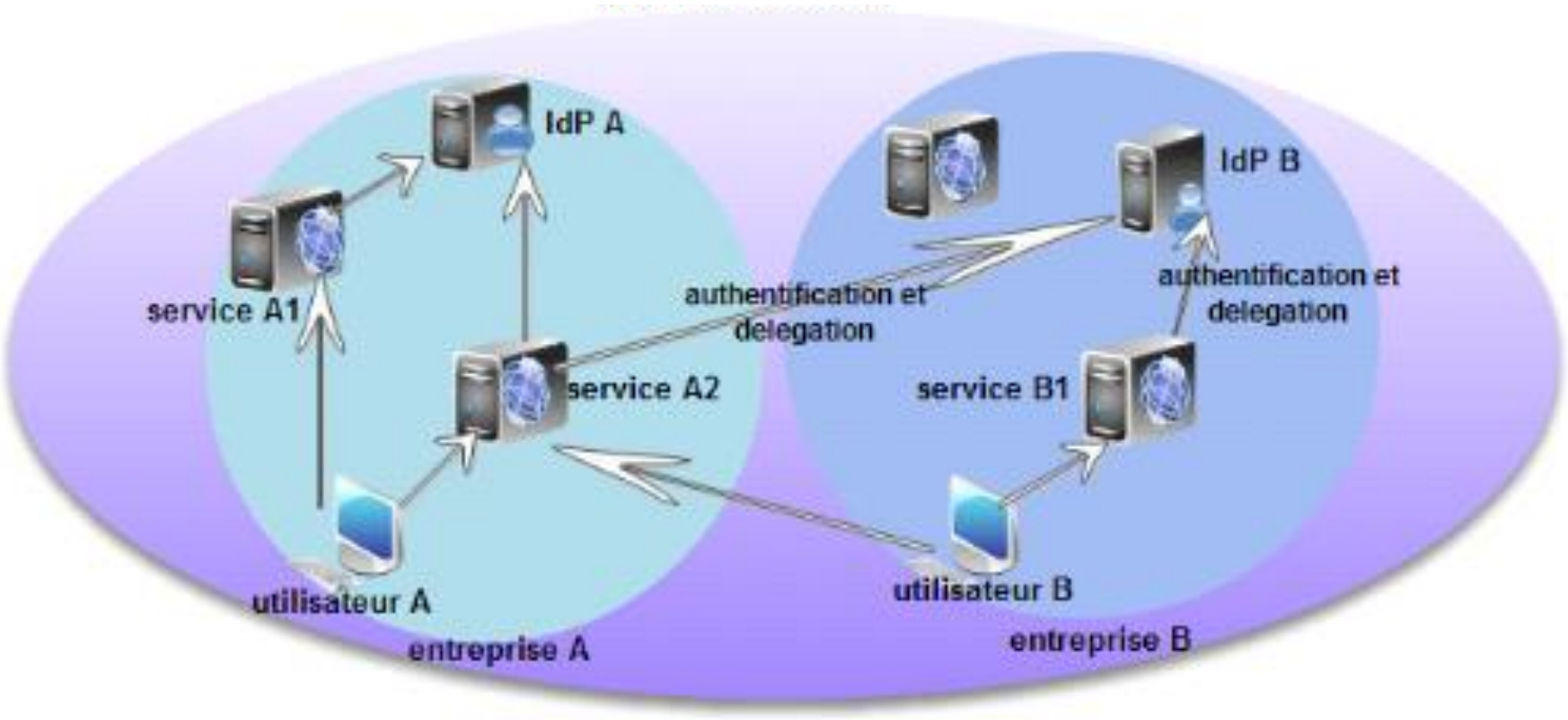
FÉDÉRATION D'IDENTITÉS

nurun
services conseils

Survol fédération

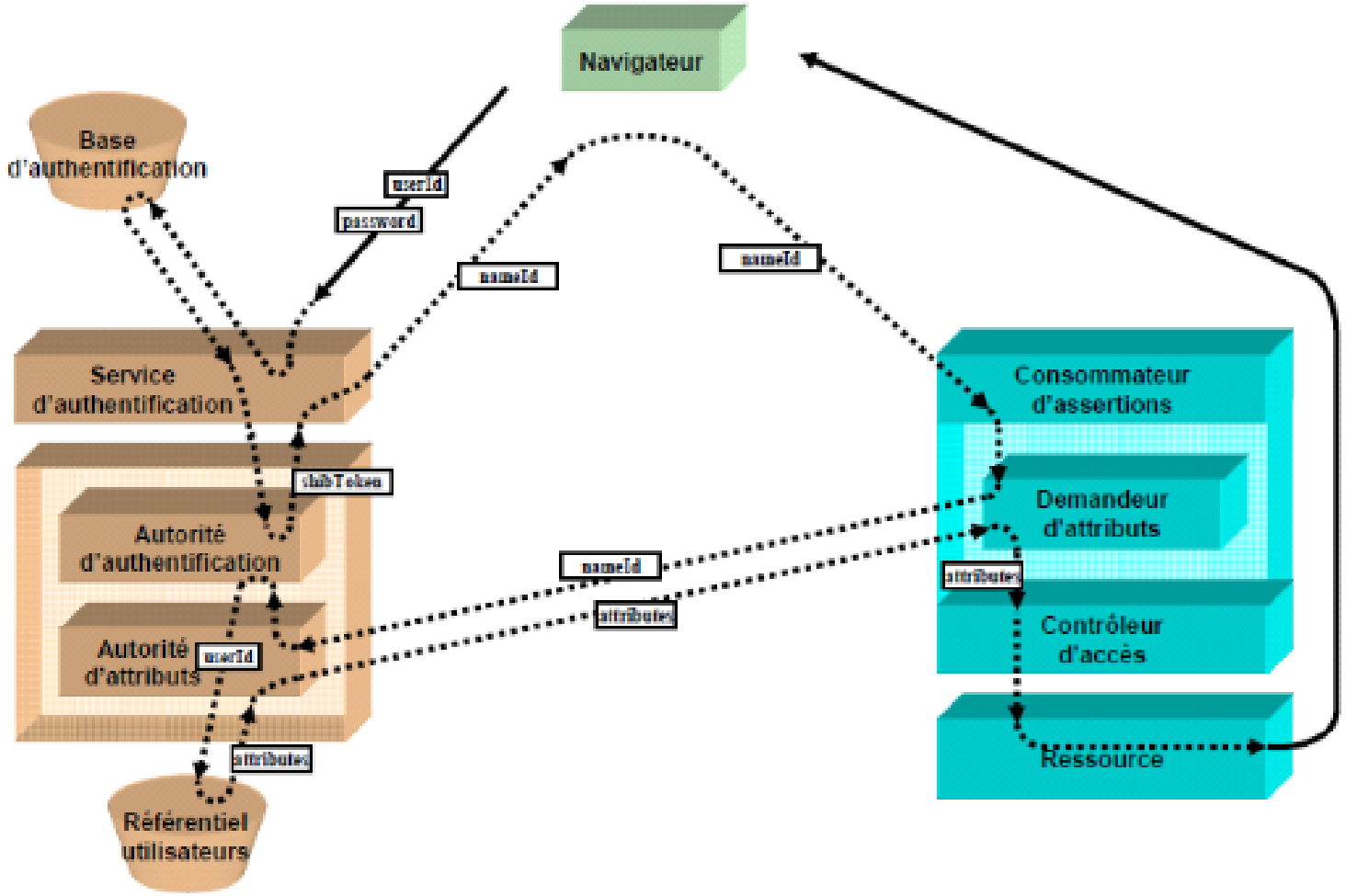
- Gestion fédérée des identités: Un modèle qui permet à plusieurs organisations d'établir un cercle de confiance dans laquelle les utilisateurs authentifiés par une organisation peuvent accéder à des ressources d'une autre organisation.
- Une fédération d'identités est la mise en application d'un tel cercle de confiance au moyen de contrats, de services et d'outils informatiques.

Cercle de confiance



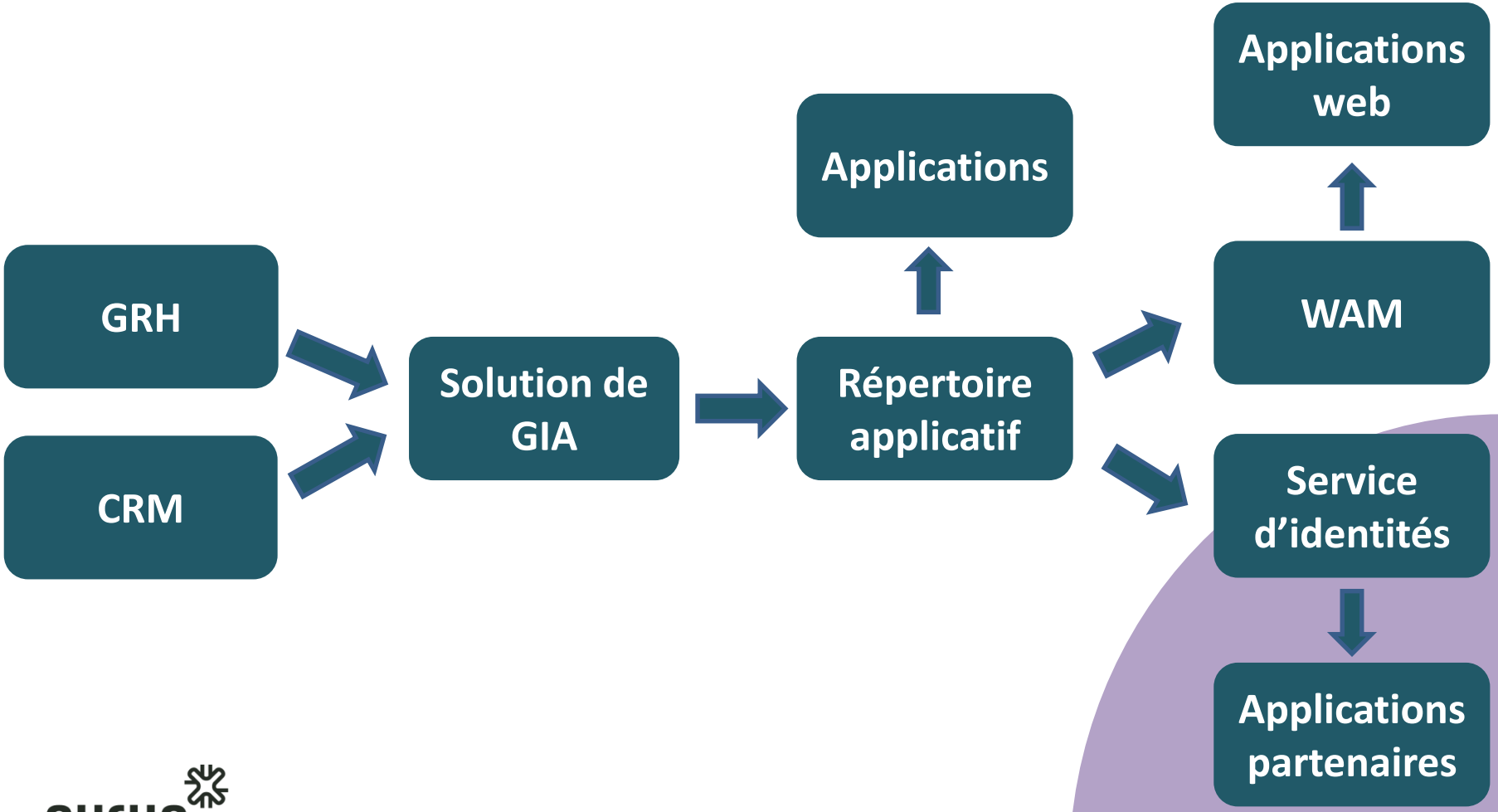
nurun
services conseils

Fédération



nuri
services conseils

Implantation Fédération



nurun
services conseils

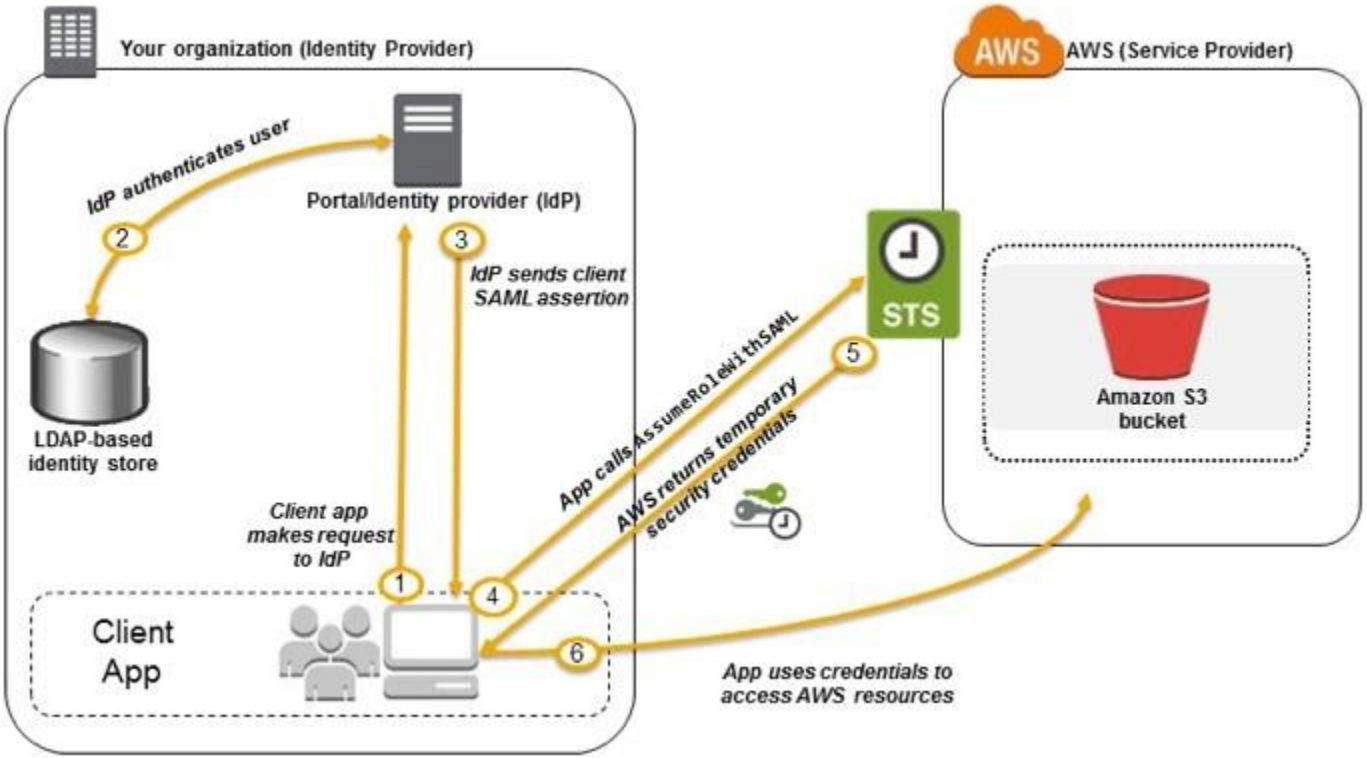
APPLICATIONS EN INFONUAGIQUE

nurun
services conseils

Survol infonuagique

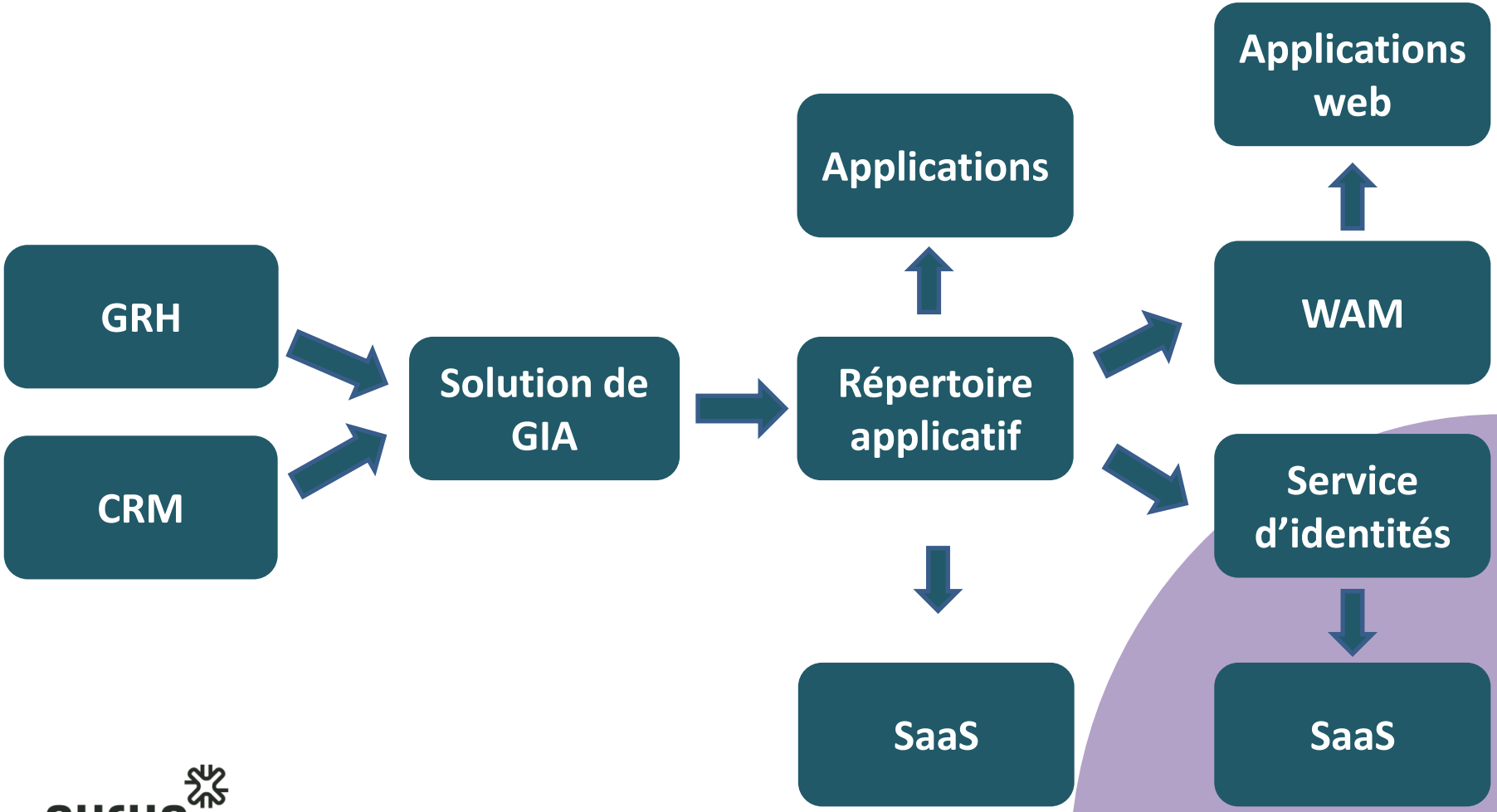
- Identification, authentification et contrôle d'accès des SaaS
- 4 modes d'opération (en ordre croissant de preference):
  - indépendant : son propre service/dépôt d'identités
  - mis à jour à partir du répertoire interne
    - Ex: AWS Directory Service, Azure AD
  - redirigé vers répertoire interne
    - Ex: Office365 fonctionne avec AD seulement
    - Ex: AWS et AD Connector
  - fédération standard
    - SAML, OpenID Connect, etc
    - Avec service interne ou public (Google, Facebook, etc)

Survol infonuagique



nurun
services conseils

Implantation infonuagique



nurun
services conseils

IAM AS A SERVICE

nurun
services conseils

IAM as a Service

- La GIA en services infonuagiques
- Ce sera pour une autre fois!

nurun
services conseils

Ça suffit pour aujourd'hui

Questions?

nurun
services conseils

Références

- ANSI INCITS 359-2004 Role Based Access Control
- NIST, « A Survey of Access Control Models », Working Draft, 2009-09-26
- NIST, Special Publication 800 -162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- OASIS, eXtensible Access Control Markup Language (XACML) TC, “Organization for the Advancement of Structured Information Standards”, Web page
- Berkeley, Enterprise Security Services Platform (ESSP) for MICROSOFT SharePoint

nurun
services conseils