From Legacy POS to Biophysical Payments: A Dual-Layer Enforcement Model for the Bio-Field-Communicator

Architectural Blueprint for POS Compatibility and Future-Proofing

The design of the Bio-Field-Communicator (BFC) is predicated on a dual-phase strategy that addresses both immediate market realities and long-term technological evolution. The primary objective is to facilitate merchant adoption of biophysical payments by creating a seamless bridge between incumbent Point-of-Sale (POS) ecosystems and an emerging biophysical-token standard . This requires a pragmatic approach that prioritizes short-term compatibility while simultaneously laying the groundwork for a standardized, vendor-neutral interface. The proposed architecture accomplishes this through a pluggable BFC module designed to integrate with existing POS kernel APIs, such as those from Verifone and Clover, which serve as a crucial gateway for initial pilots and market entry [23] [35] . These terminals, which already support software-based payment acceptance solutions like SoftPOS, represent a fertile ground for introducing biophysical capabilities without necessitating costly hardware overhauls for merchants [24] [35] . The BFC is envisioned as a foreground service running on the user's AI companion device, acting as the sole agent authorized to communicate with POS terminals . It listens for near-field triggers, hydrates the necessary user data from their `qpudatashard`, and makes a decision to Allow, Deny, or Defer a transaction based on a comprehensive set of safety and rights-enforcement rules . By presenting itself to the POS system as an enhanced conventional payment method, augmented with a minimal consent and rights envelope, the BFC minimizes friction for merchants who would otherwise have to overhaul their entire payment processing workflow .

To achieve this integration, the BFC must be mapped to the specific extension points and plugin specifications of target POS platforms. For instance, Verifone's Vx820 Duet terminal supports industry-standard communication protocols, suggesting that a BFC module could be developed to interface via TCP/IP with its integrated payment application framework [36] . Similarly, Clover's open-kernel architecture provides well-defined hooks for third-party applications, making it a prime candidate for a dedicated

BFC plugin [23] . The development process would involve creating wrappers or adapters that translate the generic BFC methods into calls conforming to the vendor-specific SDKs. This approach ensures that the core logic of the BFC remains independent of any single vendor's implementation, promoting reusability and simplifying maintenance. High-priority research actions at this stage include obtaining detailed documentation for these POS kernels, particularly for PCI CPoC (Contactless Payment on Contact Terminal) certification, which sets the baseline for secure contactless transactions . By understanding the precise entry points for initiating a payment, handling responses, and managing security contexts, developers can construct a robust and compliant BFC module. The goal is to create a "drop-in" solution where the merchant simply needs to install the BFC plugin alongside other payment methods like credit card or mobile wallets, thereby treating biophysical payments as just another option in their menu of accepted transactions .

While short-term success hinges on compatibility, the long-term vision is to establish a biophysical-token interface standard that transcends any single vendor. The real-world pilot deployments conducted using the BFC-compatible terminals will be invaluable in this regard. These pilots will generate empirical data on transaction patterns, error conditions, and merchant operational needs, which can then be distilled into a minimal, vendor-neutral specification . The process involves identifying the absolute minimum set of fields required by merchants for risk assessment, reconciliation, and dispute resolution. This curated list forms the basis of the `BfcToken.v1` schema, a simplified view of the user's biophysical state designed specifically for merchant consumption . By focusing on essential business data—such as a pseudonymous wallet identifier, interface type, consent status, and key metrics—while deliberately omitting sensitive biophysical details, the BFC ensures both utility and privacy . This standardization effort is critical for fostering a competitive and innovative ecosystem around biophysical payments. Once defined, any future terminal manufacturer can build support for this standard, confident that their hardware will be compatible with all BFC-enabled devices, thus accelerating market adoption beyond the confines of early-adopter POS systems. This phased approach, moving from targeted compatibility to broad standardization, represents a strategic pathway for introducing a transformative technology into a conservative but vital commercial infrastructure. It balances the need for practical, near-term deployment with the ambition of creating a new, equitable digital economy built on a foundation of neurorights and biosafety.

Component	Short-Term Strategy (Compatibility)	Long-Term Strategy (Standardization)
POS Integration	Develop pluggable BFC modules for Verifone/Clover/SoftPOS kernels using their existing API extension points [23] [35] .	Define a vendor-neutral biophysical-token interface standard derived from pilot data.
Merchant Experience	Treat biophysical payment as a familiar "payment method" with an added consent/rights object, requiring no workflow changes .	Terminals support a minimal `BfcToken.v1` schema, enabling interoperability across brands .
Primary Goal	Enable merchant pilots and gather real-world data with minimal friction .	Create a scalable, competitive ecosystem for biophysical payments independent of POS vendors .
Key Output	BFC plugin for specific POS kernels (e.g., Verifone, Clover).	Formal `BfcToken.v1` specification document in ALN .

This architectural blueprint demonstrates a clear and deliberate path forward. It acknowledges that innovation cannot occur in a vacuum; it must be grounded in the existing realities of the market. By first proving the concept within established POS frameworks, the project builds a case for value and reliability. Subsequently, the lessons learned are used to codify a standard that can liberate the technology from proprietary constraints, paving the way for a truly open and accessible biophysical economy.

The Dual-Layer Enforcement Model: Compile-Time Guarantees and Runtime Guard Logic

The core of the Bio-Field-Communicator's (BFC) design lies in its robust enforcement model, which combines the strengths of static analysis at compile time with dynamic validation at runtime. This dual-layer approach is fundamental to achieving the twin goals of ensuring biosafety and upholding neurorights. At the lowest level, the system leverages the strong type systems inherent in Rust and the Abstract Language Notation (ALN) used for defining shards. This compile-time layer acts as the first line of defense, architecturally preventing the creation of invalid or unsafe configurations. The principle is to make unsafe states unrepresentable in the code itself . For example, data structures representing user corridors or consent envelopes are designed so that they cannot be instantiated without including mandatory neurorights guarantees, such as `noexclusionbasicservices` and `noscorefrominnerstate` . This means that any attempt to create a transaction context lacking these fundamental protections would result in a compilation failure, catching policy violations before the code is ever deployed. Furthermore, types representing quantitative measures like risk (`RoHBound`) or environmental impact (`EcoImpactScore`) are constrained to bounded ranges, for instance, normalizing scores to a 0-1 scale to prevent logical errors or malicious manipulation of values . This rigorous type discipline transforms abstract ethical principles into concrete, enforced data models, embedding safety directly into the fabric of the system.

On top of this statically safe foundation, a second layer of enforcement operates at runtime through specialized guard modules. These guards, such as the `AugFingerprintGuard` and a future `BfcGuard`, act as the final arbiters of a transaction's legitimacy . When the BFC receives a payment request, it invokes the appropriate guard, which performs a series of dynamic checks against the user's current state and the transaction parameters. These checks are not limited to predefined schemas but encompass the active enforcement of temporal and contextual constraints. The guard logic verifies that the AI consent state is definitively `Confirmed`, ensuring that the transaction has explicit authorization . It also rigorously enforces operational caps, such as maximum prompts per hour, maximum payments per hour, daily spending limits, and acceptable latency tolerances, to prevent abuse or excessive cognitive load on the user . Critically, the runtime guard is responsible for validating the user's position relative to their health corridors, such as the `HealthyEngagementBand` and `FatigueIndex` band, refusing any transaction that would push them outside of a safe operating zone . This dynamic validation provides the necessary flexibility to respond to the user's real-time state, complementing the rigid, pre-approved structure provided by the compile-time type system.

The synergy between these two layers creates a powerful and resilient security framework. The compile-time layer ensures that the underlying data structures are always valid and aligned with core policies, providing a solid guarantee of structural integrity. The runtime guard layer adds a crucial dimension of behavioral validation, checking for compliance with dynamic constraints and contextual rules that cannot be fully captured in a static schema. Together, they form a comprehensive defense mechanism. The `EqualityPaymentGuard`, for instance, is part of this suite of runtime checks, ensuring that basic services are not denied based on a user's biophysical characteristics . The interaction between these components is orchestrated by the BFC service, which hydrates the necessary shard data from the user's `qpudatashard` and passes it to the guard for evaluation . The guard then processes this information and returns a simple, deterministic decision—Allow, Deny, or Defer—along with a structured audit record detailing the rationale for its decision . This clean separation of concerns, where complex safety logic is encapsulated within reusable guard modules, promotes modularity and maintainability. It allows for the easy addition of new guards in the future to address emerging risks or incorporate new neurorights, all while maintaining a consistent interface for the POS kernel. This dual-layer model is therefore not merely a technical detail but a central pillar of the BFC's identity, providing a robust and trustworthy mechanism for bridging the gap between human neurobiology and financial transactions.

Tokenized Grammar and Data Presentation for Merchant Adoption

A critical challenge in designing the Bio-Field-Communicator (BFC) is translating the rich, multi-faceted internal state of an augmented citizen into a simple, digestible format for merchant terminals. The solution lies in a carefully designed, multi-view tokenized grammar that separates the comprehensive internal data model from a minimalist external presentation tailored specifically for business use cases. Internally, the system relies on a detailed set of `qpudatashards`, including the `AugFingerprintShard`, `Bio-Linking shard`, and `neurorights envelopes` . These shards contain the full spectrum of information necessary for the host device to manage the user's biophysical state, consent corridors, and environmental impact metrics. Exposing this entire dataset to a merchant terminal would be impractical, insecure, and unnecessary, potentially overwhelming the merchant with irrelevant or sensitive data . Therefore, the BFC implements a crucial abstraction layer that curates this internal state into a thin, purpose-built view known as `BfcToken.v1`.

The `BfcToken.v1` schema is the cornerstone of the BFC's strategy for merchant adoption. Defined in ALN, this minimal token contains only the fields deemed essential for risk assessment, reconciliation, and dispute handling . Its design is guided by the principle of data minimization, ensuring that merchants receive exactly what they need to conduct business securely, without being exposed to personal health information or biophysical signals [14]. The fields within `BfcToken.v1` are explicitly chosen to provide verifiable, business-critical context for each transaction. This includes a pseudonymous `walletdid` to identify the user's account without revealing their identity, and an `interfacetype` field (e.g., `implantednfc`) to specify the nature of the interface being used . Crucially, the token also carries flags indicating the current consent and corridor state, such as `AiConsentState` and boolean flags confirming that prompt and payment caps have not been exceeded . This provides the merchant with assurance that the transaction adheres to the user's configured safety limits. Additionally, the token exposes economic context flags like `eco` metrics (e.g., `EcoImpactScore band`), accessibility indicators (`Eaccessibility`), and service classification (`ServiceClassBasic`), which can inform pricing or eligibility decisions .

Furthermore, the `BfcToken.v1` explicitly includes the neurorights guarantees that the user has opted into, such as `noexclusionbasicservices` and `noscorefrominnerstate` . This serves a dual purpose: it provides the merchant with transparent information about the legal and ethical framework governing the transaction, and it acts as a binding commitment that the BFC's runtime guards are programmed to enforce. By making these rights explicit and machine-readable, the token transforms abstract legal concepts into tangible, enforceable properties of the transaction itself. This approach significantly lowers the barrier to adoption for merchants, as it avoids introducing novel or confusing data formats. Instead, it presents a familiar concept—a payment token—with a few additional, well-defined attributes. The distinction between the rich internal shard and the simplified external token mirrors the relationship between a comprehensive medical file and a summary report shared with an employer; both contain relevant information, but the latter is stripped of sensitive details and tailored to a specific professional context. This careful curation of data is essential for building trust with merchants and regulatory bodies alike, demonstrating a mature understanding of data governance and privacy protection. The `BfcToken.v1` schema, therefore, is not just a technical artifact but a strategic instrument for market entry, designed to balance the need for transparency and safety with the practical demands of commercial operations.

Field Name	Type	Description	Purpose
`walletdid`	Pseudonymous DID	A decentralized identifier bound to the user's wallet, anchored via DID/Bostrom protocol .	Identifies the payer for accounting and reconciliation without exposing personal identity.
`interfacetype`	Enum	Specifies the type of biophysical interface, e.g., `implantednfc`, `EcoNFC` .	Provides context on the payment method used for routing and analytics.
`aiconsentstate`	State Machine	Represents the AI-companion's determination (e.g., CONFIRMED, DENY, SUSPENDED) .	Confirms the user's explicit intent for the transaction.
`caps_ok`	Object	Contains boolean flags for various operational limits, e.g., `maxpromptsperhour`, `maxpaymentsperhour` .	Assures the merchant that transactional activity is within user-defined safety bounds.
`ecoflags`	Object	Includes bands for `EcoImpactScore`, `Eaccessibility`, and `ServiceClassBasic` .	Provides context on the transaction's environmental and social impact for eco-rewards or pricing.
`neurightsflags`	Object	Explicitly lists granted rights, such as `noexclusionbasicservices` and `noscorefrominnerstate` .	Communicates the legally-binding neurorights framework governing the transaction.

This structured, minimal approach to data presentation is fundamental to the BFC's mission. It ensures that the technology is not only safe and ethically sound but also commercially viable and easy to integrate into existing business processes.

Enforcing Neurorights and Biosafety Through Code

The Bio-Field-Communicator (BFC) is fundamentally a framework for translating abstract neurorights principles into concrete, enforceable technical specifications. Emerging legal and ethical frameworks, such as Chile's pioneering "neurorights" law and academic proposals for a new human rights framework in the age of neuroscience, provide the conceptual underpinning for this work [16] [17] [41] . The BFC's architecture operationalizes these principles, moving them from theoretical discussions to practical, code-level implementations that protect the cerebral and mental domain of users [17] . The system is designed to uphold several key invariants derived from these foundational rights. One of the most critical is the guarantee of non-exclusion from basic services. The BFC's runtime guards are explicitly programmed to check for this condition, ensuring that a person cannot be denied access to essential goods or services simply because their biophysical state, lack of a specific implant, or adherence to certain neurorights would make them ineligible for a transaction . This prevents the emergence of a "neuro-divide," where access to society is contingent on one's biological or technological makeup.

Another cornerstone of the BFC's design is the principle of `noscorefrominnerstate`. This neuroright mandates that an individual's inner state—whether conscious thought, subconscious neural activity, or physiological signals—cannot be used to generate a score that affects their standing in society, such as a credit score or behavioral rating [7] . The BFC enforces this rule through its strict data minimization strategy. The system is architected to transmit only a pseudonymous `walletdid` and a set of pre-approved, normalized metrics to the merchant terminal . Raw biophysical data, such as EEG or EMG signals, is never exposed to the POS environment. Instead, this data is processed locally by the user's AI companion, which computes a very coarse consent state machine (CONFIRMED/DENY/SUSPENDED) and corridor flags (e.g., inside/outside `HealthyEngagementBand`) . These abstracted representations of the user's state are then sent to the POS, effectively decoupling the transaction from any interpretation of the user's internal condition. This approach aligns with expert recommendations for ethical guidelines for consumer neurotechnologies, which call for robust data governance to protect mental privacy [8] [10] .

The concept of non-coercion is also deeply embedded in the BFC's logic. Guard mechanisms enforce strict temporal constraints, such as timeouts and prompt caps, to prevent any interaction pattern that could be perceived as coercive or manipulative . For example, the system would refuse to initiate a payment if it detects that the user is in a high-stress state or if the prompt density exceeds a predefined threshold, even if the user's overall consent state is positive. This respects the user's autonomy and prevents exploitation of vulnerable moments. Furthermore, the BFC's architecture is designed to operate safely within established radiation and biosafety envelopes. NFC, the presumed physical layer for communication, is inherently low-power and radiates energy primarily as a magnetic field over very short distances, minimizing potential exposure . The BFC's configuration parameters, stored in ALN shards, explicitly forbid any settings that would exceed standard NFC power levels or dwell times, ensuring that the system remains compliant with existing safety regulations . By combining compile-time type safety, which forbids dangerous fields like `torque` or `stim` from being part of the token grammar, with runtime guard logic that validates dynamic constraints like corridor adherence and consent timing, the BFC creates a comprehensive, multi-layered defense against harm . This systematic translation of neurorights into code provides a powerful model for how technology can be designed not just to comply with laws, but to actively promote and protect fundamental human rights in the face of rapid technological change.

Auditability and Reconciliation in the Biophysical Economy

In any financial system, robust audit trails and clear reconciliation processes are non-negotiable requirements for merchants, regulators, and consumers. The Bio-Field-Communicator (BFC) addresses this necessity by generating structured, machine-readable audit records for every transactional event, aligning its internal logging mechanisms with the external needs of the merchant ecosystem. The BFC's output extends far beyond a simple Allow/Deny decision; it produces a comprehensive audit trail that captures the context and rationale behind every choice made by its safety and rights-enforcement logic . This audit trail is meticulously designed to provide the necessary information for chargebacks, dispute resolution, and routine reconciliation. The generated records are analogous to traditional `ConsentAuditRecord`s, but are enriched with data specific to the biophysical context, such as the user's `AiConsentState`, whether operational caps were respected, and the status of their health corridors at the time of the transaction .

This detailed logging is directly traceable to the requirements of merchant services. For instance, in the event of a disputed transaction, the audit record would provide irrefutable evidence that the transaction was authorized only after the user's AI companion confirmed a `Confirmed` consent state and verified that all safety caps were within acceptable limits . This shifts the burden of proof away from the merchant and onto the verifiable log generated by the BFC itself. The audit trail also incorporates the Paycomp ecosafety rails, logging sub-cent USD accounting, K/E/R scoring, and governance corridors [1] [25]. This means that every transaction contributes to a transparent ledger of both its financial and environmental impact. For merchants participating in eco-conscious programs, this data is invaluable. It allows them to track their own performance against sustainability goals and to reward customers for environmentally beneficial behaviors, such as recycling or using biodegradable devices, which are tracked via Bio-Linking hooks [1] [25]. The `eco delta` logged with each transaction quantifies the net environmental benefit or cost, providing a concrete metric for these programs [1].

The BFC's design ensures that this rich audit data is presented to the merchant in a structured format that is compatible with their existing systems. The `BfcToken.v1` schema, while minimal, is designed to include all fields necessary for basic reconciliation, such as the pseudonymous `walletdid` and transaction amount . The more detailed audit logs, however, are likely transmitted separately, perhaps through a secure web-service API that the POS terminal can call periodically to upload its transaction history and associated logs [29]. This architecture allows merchants to continue using their preferred accounting and dispute-resolution software, which can be updated to parse the new fields within the BFC's audit records. The alignment of the BFC's logging capabilities with merchant needs is a critical aspect of its design. By anticipating and fulfilling these requirements, the BFC eliminates a major barrier to adoption. Merchants can see biophysical payments not as a source of complexity and risk, but as a secure, auditable, and even beneficial addition to their payment offerings. This focus on auditability and reconciliation demonstrates a mature understanding of commercial realities and is essential for building the trust needed to integrate a disruptive new technology into the global financial system.

Log Type	Key Fields Included	Merchant Use Case
`ConsentAuditRecord`	`walletdid`, `transaction_id`, `timestamp`, `aiconsentstate`, `decision_reason` (e.g., caps exceeded, out of corridor)	Dispute resolution, chargeback justification, verification of user consent.
`K/E/R Scoring Log`	`k_score`, `e_score`, `r_score`, `transaction_id`, `timestamp` [25]	Risk assessment, fraud monitoring, loyalty program tracking.
`Eco-Delta Log`	`eco_delta_kwh`, `device_hours_saved`, `recycling_credit`, `transaction_id`, `timestamp` [1]	Sustainability reporting, participation in eco-reward programs, environmental impact analysis.
`Biophysical Cost Log`	`decoder_accuracy`, `avg_latency_ms`, `fatigue_index`, `healthy_engagement_band_status`	System optimization, user wellness tracking, tuning payment flows to minimize strain.

This systematic approach to auditing and logging ensures that the BFC is not a "black box" but a transparent and accountable system. It provides the necessary tools for all stakeholders—merchants, users, and regulators—to verify that transactions are conducted fairly, safely, and in accordance with established neurorights and biosafety standards.

Actionable Roadmap for BFC Development and Standardization

To transition the Bio-Field-Communicator (BFC) from a conceptual framework to a deployable solution, a series of concrete, actionable steps are required. These steps are designed to formalize the BFC's architecture, define its interfaces, and validate its utility against real-world merchant needs. The first and most critical action is to draft the formal `BfcToken.v1` schema in ALN. This document will serve as the definitive specification for the minimal, merchant-facing token grammar . It must precisely define each field—its name, data type, and whether it is mandatory or optional. This schema will be the foundation upon which the vendor-neutral biophysical-token standard is built, ensuring that any future terminal capable of supporting the BFC will have a clear and unambiguous contract to adhere to . The development of this schema should be informed by a thorough review of the internal `qpudatashard` structures to ensure that the external view accurately reflects the user's state without exposing raw biophysical data .

Concurrently, the BFC's application programming interface (API) for POS systems must be specified. This involves defining a simple Rust trait or a C-compatible function interface that encapsulates the BFC's core functionality . This interface should consist of a small number of essential methods, such as `init()`, `evaluate_payment(BfcToken, Amount) -> Decision`, and `flush_audit()`. This "contract" will act as the blueprint for developing the specific wrappers and plugins needed to integrate the BFC with different POS kernels, such as those from Verifone and Clover . By standardizing this interface, developers can create platform-specific implementations while ensuring that the core logic of the BFC remains consistent and portable. The next step involves a deep dive into the developer documentation and SDKs of target POS platforms to map these BFC methods to the actual extension points available in their systems . This technical due diligence is crucial for identifying any potential integration challenges and for estimating the effort required for development.

Finally, a comprehensive audit of merchant requirements is necessary to close any gaps between the BFC's output and the needs of the commercial world. This involves cross-referencing the fields included in the `BfcToken.v1` schema and the content of the generated audit records with the specific data points required by merchants for chargebacks, receipt generation, and daily reconciliation . Any missing information identified through this process must be addressed by augmenting the `BfcToken.v1` schema or the audit log format. For example, if merchants require a unique transaction ID for every settlement batch, this field must be added to the schema. This iterative process of specification, mapping, and validation ensures that the BFC is not only technologically advanced and ethically sound but also practically useful and commercially viable. By following this roadmap, the project can systematically build a robust, standardized, and trusted payment service that successfully bridges the gap between today's POS terminals and the future of biophysical commerce.

Reference

1. Zoznam publikácií zo stránok EP Think Tank https://www.europarl.europa.eu/thinktank/sk/research/advanced-search/pdf?keywords=36
2. VAJIRAM AND RAVI The Recitals (July 2024) Page 1 https://vajiram-prod.s3.ap-south-1.amazonaws.com/Cover_Page_Recitals_merged_dc942de231.pdf
3. Vision IAS Current Affairs Monthly Magazine August 2025 ... https://www.scribd.com/document/915330415/Vision-IAS-Current-Affairs-Monthly-Magazine-August-2025-PDF
4. Artificial Intelligence in Science and Society: The Vision of ... https://ieeexplore.ieee.org/iel8/6287639/10820123/10839366.pdf
5. Artificial Intelligence - Springer Link https://link.springer.com/content/pdf/10.1007/978-3-031-92973-1.pdf
6. Artificial and Spiritual Intelligence: Proceedings of the 2023 ... https://www.researchgate.net/publication/394025530_Artificial_and_Spiritual_Intelligence_Proceedings_of_the_2023_Conference_of_the_International_Society_for_Science_Religion
7. Written feedback after 4th ERPB technical session (cross ... https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov221205_writtenfeedback.en.pdf
8. Protecting Brain Privacy in the Age of Neurotechnology https://www.researchgate.net/publication/384971350_Protecting_Brain_Privacy_in_the_Age_of_Neurotechnology_Policy_Responses_and_Remaining_Challenges

9. (PDF) Neurorights, Mental Privacy, and Mind Reading https://www.researchgate.net/publication/382079309_Neurorights_Mental_Privacy_and_Mind_Reading
10. Towards a Governance Framework for Brain Data https://arxiv.org/pdf/2109.11960
11. 1 Cyber Risks to Next-Gen Brain-Computer Interfaces https://arxiv.org/pdf/2508.12571
12. (PDF) NEUROLAW-Legal Impacts of Neurotechnology https://www.researchgate.net/publication/390237085_NEUROLAW-Legal_Impacts_of_Neurotechnology
13. The Impact of Artificial Intelligence on Human Thought https://arxiv.org/pdf/2508.16628
14. The ethical and legal landscape of brain data governance https://www.researchgate.net/profile/Damian-Eke/publication/366683964_The_ethical_and_legal_landscape_of_brain_data_governance/links/63b0b377097c7832ca7da5ee/The-ethical-and-legal-landscape-of-brain-data-governance.pdf
15. Upgrading the protection of children from manipulative and ... https://arxiv.org/pdf/2207.09928
16. Towards new human rights in the age of neuroscience and ... https://www.researchgate.net/publication/316473442_Towards_new_human_rights_in_the_age_of_neuroscience_and_neurotechnology
17. Common human rights challenges raised by different ... https://www.researchgate.net/publication/356412675_COMMON_HUMAN_RIGHTS_CHALLENGES_RAISED_BY_DIFFERENT_APPLICATIONS_OF_NEUROTECHNOLOGIES_IN_THE_BIOMEDICAL_FIELD
18. Arxiv今日论文 | 2026-01-09 http://lonepatient.top/2026/01/09/arxiv_papers_2026-01-09.html
19. Dissociating language and thought in large language models https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613(24)00027-5
20. Dragon-book.pdf https://faculty.sist.shanghaitech.edu.cn/faculty/songfu/cav/Dragon-book.pdf
21. (PDF) ACTG-ARL: Differentially Private Conditional Text ... https://www.researchgate.net/publication/396747253_ACTG-ARL_Differentially_Private_Conditional_Text_Generation_with_RL-Boosted_Control
22. PROVAL: A framework for comparison of protein sequence ... https://www.sciencedirect.com/science/article/pii/S2772415822000128
23. The (not-so) silent takeover: https://www.capgemini.com/wp-content/uploads/2025/09/WPR_2026_4e6d5a.pdf

24. Document 1083376791 | PDF https://www.scribd.com/document/665217604/document-1083376791
25. Contactless Card Pos Machine(999+) https://www.alibaba.com/showroom/contactless-card-pos-machine.html
26. Credit Card Swipe Tablet - Portable & Efficient Solutions https://m.alibaba.com/showroom/credit-card-swipe-tablet.html
27. 333333 23135851162 the 13151942776 of 12997637966 ftp://ftp.cs.princeton.edu/pub/cs226/autocomplete/words-333333.txt
28. Insight MFR Names https://bidopportunities.iowa.gov/Home/ShowContractDocument/233de3c6-b20e-480c-a6f0-92e3176d4eb2
29. Tools and Solutions for Modernizing Your IBM i Applications https://www.redbooks.ibm.com/redpapers/pdfs/redp5095.pdf
30. notebookf0cca14682 https://www.kaggle.com/code/drnikolas6/notebookf0cca14682
31. Words | PDF | Science | Engineering https://www.scribd.com/doc/88199361/Words
32. Opportunities and Challenges for Machine Learning-Assisted ... https://pubs.acs.org/doi/10.1021/acscentsci.3c01275
33. Code Generation in Computational Neuroscience https://www.frontiersin.org/journals/neuroinformatics/articles/10.3389/fninf.2018.00068/full
34. Toward large reasoning models: A survey of reinforced ... https://www.cell.com/patterns/fulltext/S2666-3899(25)00218-1
35. SoftPOS and PCI MPoC Certification Demystified https://eazypaytech.com/softpos-and-pci-mpoc-certification-demystified/
36. Using Electronic Cash Register interface to communicate ... https://stackoverflow.com/questions/51671036/using-electronic-cash-register-interface-to-communicate-with-credit-card-termina
37. EMVCo Payment Tokenisation Specification Technical ... https://www.scribd.com/document/373734735/EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2-0-pdf
38. (PDF) Emotion Classification Based on Biophysical Signals ... https://www.researchgate.net/publication/338118399_Emotion_Classification_Based_on_Biophysical_Signals_and_Machine_Learning_Techniques
39. Generative AI: A systematic review using topic modelling ... https://www.sciencedirect.com/science/article/pii/S2543925124000020
40. Foundation models and intelligent decision-making https://www.cell.com/the-innovation/fulltext/S2666-6758(25)00151-1

41. First Win for the Neurorights Campaign: Chile plans to ... https://www.researchgate.net/publication/357735170_First_Win_for_the_Neurorights_Campaign_Chile_plans_to_regulate_all_neurotech_and_ban_the_sale_of_brain_data
42. Udemy For Business Course List | PDF | Sustainability https://www.scribd.com/document/821166664/Udemy-for-Business-Course-List
43. List of All | PDF https://www.scribd.com/document/643019297/list-of-all-xlsx
44. Skills | PDF https://www.scribd.com/document/819588329/Skills
45. Release notes https://docs.adyen.com/point-of-sale/firmware-release-notes